
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**IMPROVING RESOURCE ALLOCATION DECISIONS TO REDUCE THE RISK OF TERRORIST ATTACKS ON PASSENGER RAIL SYSTEMS**

by

Lawrence W. King

December 2016

Thesis Co-Advisors: Thomas Mackin
Rudy Darken

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 |
|---|---|---|---|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503. | | | |
| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** December 2016 | **3. REPORT TYPE AND DATES COVERED** Master's thesis | |
| **4. TITLE AND SUBTITLE** IMPROVING RESOURCE ALLOCATION DECISIONS TO REDUCE THE RISK OF TERRORIST ATTACKS ON PASSENGER RAIL SYSTEMS | | | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S)** Lawrence W. King | | | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943-5000 | | | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | | | **10. SPONSORING / MONITORING AGENCY REPORT NUMBER** |
| **11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____. | | | |
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release. Distribution is unlimited. | | | **12b. DISTRIBUTION CODE** |

**13. ABSTRACT (maximum 200 words)**

Passenger rail systems continue to be a prime target for terrorists. Since 1995, there have been hundreds of attacks targeting assets worldwide that have resulted in almost 1,000 deaths and more than 1,500 injuries. As evidenced by the March 2016 attack in Brussels, Belgium, the openness and accessibility of passenger rail facilities are attractive to adversaries. This thesis reviews the current approach to risk assessment used by system operators to counter threats and proposes a new model to improve resource allocation decisions, which is intended to reduce the risk of terrorist attacks on passenger rail. The use of the game theory attacker-defender methodology in deciding where to allocate security improvements will increase the security of systems in defending against attacks. Changing tactics require security professionals to continually enhance the security posture of rail systems to deter terrorists. Limited resources make the job of securing a passenger rail system more of a challenge today than ever before.

| **14. SUBJECT TERMS** passenger rail security, decision making, risk assessment, rail systems, metro, mass transit, subway, risk management, game theory, passenger rail bombing, attacker-defender methodology | | | **15. NUMBER OF PAGES** 103 |
|---|---|---|---|
| | | | **16. PRICE CODE** |
| **17. SECURITY CLASSIFICATION OF REPORT** Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified | **20. LIMITATION OF ABSTRACT** UU |

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

# IMPROVING RESOURCE ALLOCATION DECISIONS TO REDUCE THE RISK OF TERRORIST ATTACKS ON PASSENGER RAIL SYSTEMS

Lawrence W. King
Supervisory Transportation Security Inspector, Department of Homeland Security,
Transportation Security Administration, New York, NY
B.S., St. John's University, 1984
M.S., St. John's University, 1989

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES**
**(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL**
**December 2016**

Approved by: Thomas Mackin
Thesis Co-Advisor

Rudy Darken
Thesis Co-Advisor

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Passenger rail systems continue to be a prime target for terrorists. Since 1995, there have been hundreds of attacks targeting assets worldwide that have resulted in almost 1,000 deaths and more than 1,500 injuries. As evidenced by the March 2016 attack in Brussels, Belgium, the openness and accessibility of passenger rail facilities are attractive to adversaries. This thesis reviews the current approach to risk assessment used by system operators to counter threats and proposes a new model to improve resource allocation decisions, which is intended to reduce the risk of terrorist attacks on passenger rail. The use of the game theory attacker-defender methodology in deciding where to allocate security improvements will increase the security of systems in defending against attacks. Changing tactics require security professionals to continually enhance the security posture of rail systems to deter terrorists. Limited resources make the job of securing a passenger rail system more of a challenge today than ever before.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AD | attacker-defender |
| APTA | American Public Transportation Association |
| CARVER | criticality, accessibility, recuperability, vulnerability, effect and recognizability |
| CPTED | crime prevention through environmental design |
| DHS | Department of Homeland Security |
| DOT | Department of Transportation |
| ERM | enterprise risk management |
| FEMA | Federal Emergency Management Agency |
| FRA | Federal Railroad Administration |
| FT | fault tree analysis |
| FTA | Federal Transit Administration |
| IED | improvised explosive device |
| IT | information technology |
| MOP | measure of performance |
| MSRAM | maritime security risk analysis model |
| NYCT | New York City Transit |
| PRA | probabilistic risk assessment |
| ROI | return on investment |
| SME | subject matter expert |
| SOP | standard operating procedure |
| TRAM | terrorist risk assessment and management |
| TSA | Transportation Security Administration |
| TSGP | Transit Security Grant Program |
| TVC | threat vulnerability consequence |

THIS PAGE INTENTIONALLY LEFT BLANK

# EXECUTIVE SUMMARY

The United States transportation network is a vast enterprise consisting of highway, air, maritime, and rail sectors. The rail sector divides into freight and passenger systems. Each one has operational characteristics, structural features, and security vulnerabilities that differentiate it from the others. Passenger rail is experiencing a revival. In 2013, there were more than 4.8 billion rail trips in the United States.[1] Approximately 11.3 million passengers in 35 metropolitan areas utilize rail transportation daily, which is the highest level of ridership since 1957.[2]

Recent worldwide attacks show that terrorists are intent on inflicting damage to passenger rail assets. This mode of transportation has characteristics, such as large numbers of riders, easy access, multiple points of entry and exit, and scheduled stops along fixed routes, that make it an attractive target for terrorism.[3] The Mineta Transportation Institute cataloged surface transportation attacks from 1970 to 2007 and found that passenger rail systems are the most common target of terrorists.[4]

The security posture of rail systems varies from system to system. A "one size fits all" approach to security is unlikely to deter terrorism so operators must choose strategies from the various categories such as technologies or visibility patrols and development of multifaceted plans that avoid interfering with functional efficiency.[5] A layered strategy, which is characterized by concentric sets of security features, exhibits the greatest potential to deter attacks. As security systems mature, new strategies develop in response to evolving threats. In some cases, these strategies overlap existing programs. Since older systems and technologies may not be effective against assailants who adapt to defeat

[1] American Public Transportation Association, "Quarterly and Annual Totals by Mode, 1990–present," accessed July 23, 2014, www.apta.co m/resources/statistics/Pages/ridershipreport.aspx.

[2] Nicholas Armstrong et al., *Securing America's Passenger Rails: Analyzing Current Challenges, and Future Solutions* (Syracuse: Maxwell School of Citizenship and Public Affairs, 2008), 18.

[3] U.S. Department of Homeland Security, *Train Station Attack Methods* (Washington, DC: Transportation Security Administration, Office of Intelligence, 2010), 3.

[4] Brain M. Jenkins and Bruce R. Butterworth, *Analysis of Terrorist Attacks against Public Transportation* (San Jose: Mineta Transportation Institute, 2007), 4.

[5] Armstrong et al., *Securing America's Passenger Rails,* 18.

procedures, modifications may be required to blend the new protocols into a security program. Sound decision making for security resource allocations is critically important. Rail systems operators should recognize that incorporating new procedures, protocols, and technology alone, without taking a systematic approach to implementation, could provide terrorists with the opportunity to take advantage of a gap and possibly defeat the entire security system.

How can passenger rail systems improve resource allocation decisions intended to reduce the risk of terrorist attacks? Rail systems use a variety of risk assessment processes. Large networks have the resources to develop complex processes, but operators of smaller networks are not as fortunate. They are subject to constraints, such as budgetary support, that restrict their ability to employ the same risk assessment programs that larger operators utilize.

Passenger rail security improvements, like other forms of infrastructure protection, require system operators to assess threats from an attack by an intelligent adversary. Response to a threat results in the development of defenses to deter attacks, or in the case of a successful attack, to enhance resiliency to mitigate the damage. Infrastructure protection against intentional acts is not like protecting against acts of nature. Intelligent adversaries will change their tactics to defeat security and exploit any vulnerabilities. Risk assessment models support game theory by providing probabilities for various attacker-defender actions.[6]

This thesis recommends game theory principles in attacker-defender methodology to guide resource allocation decisions for passenger rail systems. Game theory is superior to other risk management approaches, which fail to consider the tendency of terrorists to react to defender strategies. Examining the threat environment and factors associated with defense against malicious actors will result in a better understanding of the assessment options available to defend against threats. Additionally, it will encourage those responsible for passenger rail security to balance the effectiveness of counter measures and resource implementation, including operational issues and costs.

[6] Louis Anthony Cox, Jr., *Improving Risk Analysis* (New York: Springer, 2012), 173.

The better option for risk assessment of deliberate threats is to model the system and then apply a worst-case analysis. Game theory models the actions of "players" and offers a more useful modeling framework. These players include a society wanting to prevent attacks against its infrastructure, adversaries who recognize protective measures and seek to attack in the most harmful way, and a system that can bounce back and operate to the best of its diminished ability.[7] The goal of game theory is to maximize the resiliency of infrastructure, which minimizes the disruption caused by worst-case attacks. It is not possible to deter all terrorist attacks so success is measured by the ability to keep the system operating. A system will act to mitigate the results of any attack and operate to the best of its reduced ability. The goal is to maximize resilience and minimize disruption against worst-case attacks.[8]

Game theory principles in the attacker-defender (AD) methodology result in effective recommendations for allocating resources because the foundation of AD is based on improved risk analyses of the actions of intelligent adversaries. It involves decision making by which participants make choices that impact on the actions of an opponent.[9] This yields well-grounded results that inform the decision maker as to the worst possible outcome, not the most probable.

For this thesis, the researcher performed and analysis on assets of the New York City Transit (NYCT) subway system to demonstrate the utility of using the attacker-defender methodology to improve resource allocation decisions for passenger rail systems. One option involved an attack focused on one station that utilized multiple attack modes. A second option targeted more than one station using the same attack mode. The measurement of the impact, or how successful the attack is in affecting the measure of performance, was reduction in ridership. The results supported the use of the AD methodology to improve decision making for resource allocations.

---

[7] David L. Alderson and Gerald Brown, "Solving Defender-attacker-defender Models for Infrastructure Defense" (paper presented at the 12th Informs Computing Society Conference, Monterey, CA, January 2011).

[8] Ibid., 29.

[9] Theodore L. Turocy, "Game Theory," in *Encyclopedia of Information Systems* (New York: Academic Press, 2002), 2.

Game theory, specifically the AD methodology, has the potential to be of use in protecting against threats from terrorists. Intentional threats are evolving rapidly as terrorists respond to defenses. When faced with an intelligent adversary who learns from the past, history offers no security, and the threat data can be too general to eliminate uncertainty. Terrorists are at liberty to change what they attack, when they attack, and how they attack at any point in time. Game theory makes for a reliable, reusable tool that system personnel nationwide can use in risk assessments for passenger rail systems. Though the features of a system may change, the general approach remains the same.

The attacker-defender methodology engages in worst-case scenarios and develops system models to determine what the worst case could be. Though this approach does not provide an ironclad prediction, it does frame the solution to what is possible through an attack by an intelligent adversary, and it shows great promise for resource allocation decisions.[10] It is apparent that rail systems have to concentrate on worst-case scenarios in assessing and reducing vulnerabilities because of the lack of confidence in reliability analyses based on unpredictable adversarial threats.

Protecting infrastructure from an attack is extremely difficult. Recommendations for protection must be grounded in an understanding of system performance and clearly describe the expected costs and benefits of a particular policy intervention. Processes and protocols have to be multi-layered, nimble, and flexible to protect against threats that try to defeat security improvements.

[10] National Research Council, *Review of the DHS Approach to Risk Analysis* (Washington DC: National Academies Press, 2010), 106.

# ACKNOWLEDGMENTS

I am in debt to the leadership of the Transportation Security Administration for nominating me to attend this program. I am certain that this experience will broaden my critical thinking skills and benefit the agency in its mission to provide secure transportation throughout the United States.

My family deserves much credit for my successful completion of this program. The time that I devoted to studying was time spent away from them. My wife, Marylou, was extremely supportive throughout the journey. My son, Larry, who by way of his own academic achievements gave me the motivation to persevere during the 18 months I spent pursuing this degree.

I sincerely thank my advisors, Dr. Thomas Mackin and Dr. Rudy Darken, engineers by trade, who coached and guided me, a security professional, throughout this program to the finish line. It was a job well done, gentlemen.

I must acknowledge my classmates, who were there to lean on and learn from as we progressed from one semester to the next. I am sure that the hard work they have expended will pay tremendous benefits down the road. I have the utmost respect for these individuals and fond memories to look back on.

Finally, to the instructors and staff at the Center for Homeland Defense and Security, you are the reason why this program has an outstanding reputation. Thank you for your dedication to excellence.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

The United States transportation network is a vast enterprise consisting of highway, air, maritime, and rail sectors. Each moves people and materials in a unique way. The rail sector divides into freight and passenger systems. There are many different types of passenger rail operations, including mass transit systems, commuter railroads, people movers, and tourist railroads. Each one has operational characteristics, structural features, and security vulnerabilities that differentiate it from the others. Vast rail networks were built as demand for affordable, reliable transportation increased across the country. The convenience of passenger rail transportation has become so commonplace that society now takes it for granted. A key characteristic that makes this mode noteworthy in the transportation sector is the ability to concentrate the flow of people.

For most of the past, passenger rail security has concentrated on traditional security methods that can be summarized in three words: guards, guns, and gates.[1] However, security strategies currently in use are grouped into one of the following domains:

- Process based such as increased visibility patrols
- Technology based including closed circuit television and
- Chemical, biological, radiological, and nuclear detection
- Facility improvements like blast resistant trash receptacles

No method alone is sufficient to ward off attacks so operators choose strategies from the categories mentioned above and develop a multi-faceted plan that does not hamper functional efficiency.[2]

A "one size fits all" security plan is unlikely to work. Rail systems vary, and the threats they face cannot be prevented by generalized law enforcement strategies alone. Any methods employed have to be integrated into operations and designed to deter

[1] National Research Council, *Deterrence, Protection, and Preparation: The New Transportation Security Imperative* (Washington DC: National Academies of Science, 2002), 1.

[2] Nicholas Armstrong et al., *Securing America's Passenger Rails: Analyzing Current Challenges, and Future Solutions* (Syracuse: Maxwell School of Citizenship and Public Affairs, 2008), 18.

terrorism. Alternately, they may enhance the ability to recover from an attack. A layered strategy, with sets of security assets providing defensive support behind each other, can effectively deter terrorist activities. Protective measures fortify the outer perimeter and progress inward focusing on the exterior, interior, and restricted access areas. Layered systems are difficult to compromise by way of a single facet, such as a gate or a guard. Additionally, each layer provides backup for the others. While a single feature may be defeated, multiple layers support impermeability.[3] Moreover, increasing the number of layers is beneficial to the defender. The defense in depth methodology is an example of a layered system. It utilizes multi-layered protections to create a system that relies on successive features instead of one security barrier.[4] Conventional strategies concentrate resources on the frontline. Defense in depth is effective against an attacker who can concentrate forces on a small number of locations in a large rail system. As adversaries attempt to penetrate, they encounter resistance designed to prevent, deter, and defeat an attack. Defense in depth can include different technologies to protect various targets.

## A. PROBLEM STATEMENT

How can passenger rail systems improve resource allocation decisions intended to reduce the risk of terrorist attacks? Much is at stake, including the protection of riders, employees, and equipment.

Transportation is integral to America. We rely on some form of transportation in most of our daily activities. One mode of transportation, passenger rail, has particular significance to the economic vitality of the United States. Millions of people in major metropolitan areas utilize this mode of transportation. The roots of passenger rail transportation date back to the establishment of the Baltimore and Ohio Rail Road in 1827.[5] Some cities like New York, Boston, and Chicago owe their development to a rail system serving the municipality around the clock.

---

[3] National Research Council, *Deterrence, Protection, and Preparation*, 2.

[4] Matthew Rosenquist, *Defense in Depth Strategy Optimizes Security* (Santa Clara, CA: Intel Corporation, 2008), http://www.itworldcanada.com/archive/WhitePaperLibrary/PdfDownloads/Defense_In_Depth_Strategy_Optimizes_Security.pdf, 4.

[5] Library of Congress, "America's Story from America's Library," accessed July 14, 2016, http://www.americaslibrary.gov/jb/nation/jb_nation_train_1.html.

Even though it is a popular form of transportation, there are serious security concerns for patrons of the rail system. Passenger rail has characteristics, such as large numbers of riders, easy access, multiple points of entry and exit, and scheduled stops along fixed routes, that make it an attractive target for terrorism.[6] The number of attacks against passenger rail systems confirms this supposition. A review conducted by the Mineta Transportation Institute in 2010 cataloged the characteristics of surface transportation attacks from 1970 to 2007 and found that passenger rail systems are the most common target.[7] The safety of people who patronize mass transit, the protection of critical infrastructure, and retention of the public's confidence in passenger rail is reliant on the security decision-making process. Many strategies have been employed and significant resources expended to secure passenger rail assets.

As security systems mature, new strategies develop in response to evolving threats. In some cases, these strategies overlap existing programs. Since older systems and technologies may not be effective against assailants who adapt to defeat procedures, modifications may be required to blend the new protocols into the program. Rail systems operators should recognize that incorporating new procedures, protocols, and technology alone, without taking a systematic approach to implementation, could provide terrorists with the opportunity to take advantage of a gap and possibly defeat the entire security system.[8]

This thesis recommends use of the game theory principles in the attacker-defender (AD) methodology to guide decision-making specific to the passenger rail industry. The goal is to encourage security personnel to weigh and balance the effectiveness of measures and their implementation, operation, and costs. Central to this process is the notion of risk management. In *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, published by the Department of Homeland Security (DHS), it states, "risk management is establishing the capacity to identify, understand, and address

---

[6] U.S. Department of Homeland Security, *Train Station Attack Methods* (Washington, DC: Transportation Security Administration, Office of Intelligence, 2010), 3.

[7] Brain M. Jenkins and Bruce R. Butterworth, *Analysis of Terrorist Attacks against Public Transportation* (San Jose: Mineta Transportation Institute, 2007), 4.

[8] National Research Council, *Deterrence, Protection, and Preparation*, 2.

complex challenges and opportunities and that risk management is the foundation for making and implementing improved homeland security decisions."[9] A report by the National Research Council further supports this contention by stating, "risk management distinguishes between and among alternative actions, assesses capabilities, and prioritizes activities and associated resources by understanding risk and its impact on their decisions."[10] Game theory methodology is relevant to rail system executives and security staff who determine implementation priorities, as well as planners who must explain the rationale for courses of action. The findings could also be helpful to government oversight agencies, such as state Departments of Transportation (DOT) and the Federal Emergency Management Agency (FEMA).

A review of previous attacks can identify the gaps that were exploited for the plots to succeed. These findings can lead to an understanding of the security apparatus that was in place on these systems at the time of the attacks. For instance, were the deficiencies related to lack of institutional knowledge or internal security policy? The information compiled from identification of these gaps defines the threat that the proposed model can be tested against. The strides that system operators have made to date in securing passenger rail transportation are commendable. This research provides a tool for rail system operators to guide security resource decision-making activities in the future.

## B. RESEARCH QUESTION

How can passenger rail systems improve resource allocation decisions intended to reduce the risk of terrorist attacks? This thesis recommends that passenger rail systems adopt the game theory methodology to meet the challenges of providing enhanced security when the threat of terrorism is on the rise.[11] As Jeremey Plant and Richard Young wrote in *Securing and Protecting America's Railroad System*, "The challenge is

[9] U.S. Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington DC: U.S. Department of Homeland Security, 2011), 8.

[10] National Research Council, *Review of the DHS Approach to Risk Analysis* (Washington DC: National Academies Press, 2010), 12.

[11] Jeremy F. Plant and Richard R. Young, *Securing and Protecting America's Railroad System: US Railroads and Opportunities for Terrorist Threats* (Harrisburg: Pennsylvania State University, 2007), 5.

how to enhance railroad service to population centers overwhelmed by a labyrinth of over-used roadways while lowering threats the railroads may face because they are attractive targets for terrorists."[12]

## C. BACKGROUND

Like any other company, a passenger rail system works diligently to minimize risk in all facets of its operation. Security and safety are important considerations in this endeavor. The analysis of various factors results in decisions on how to effectively implement security improvements. It is not accomplished in a haphazard fashion but rather through a series of steps that have been tested and affirmed as procedurally sound.

Risk management is a comprehensive systematic evaluation of risk and careful, planned application of countermeasures to improve organizational security.[13] The goal is to enable local decision makers to manage risk and to identify measures that provide a high return on investment (ROI) in responding to the challenges that confront passenger rail operations. In *Emergency Preparedness for Transit Terrorism*, Annabelle Boyd and John Sullivan define a risk assessment as a

> comprehensive study of a rail agency to identify components most vulnerable to damage and to assess the impact such activity on a system. The results of a risk assessment aid officials in making critical decisions concerning the allocation of available resources such as where to harden assets, change procedures, or assign personnel to reduce the risk.[14]

The principles of security and safety are often intermingled. Transportation safety deals with the prevention of accidents, such as slips, trips, and falls. On the other hand, security deals with the prevention or mitigation of harmful actions to people or property. Consequently, a security risk assessment is different from a safety assessment. A safety assessment evaluates the provisions in place to determine if the risk of an injury is as low

---

[12] Ibid., 58.

[13] U.S. Department of Homeland Security, *Vulnerability Assessment Methodologies Report* (Washington DC: Office for Domestic Preparedness, 2003), 9.

[14] Annabelle Boyd and John P. Sullivan, *Emergency Preparedness for Transit Terrorism* (Washington DC: National Academies Press, 1997), 29.

as reasonably achievable.[15] Although they are two different regimens, in some cases enhancements to safety provide ancillary benefits to security, just as improvements to security supplement safety. There is a similar relationship between terrorism and crime. Mitigation strategies to deter terrorism have a direct impact on crime, and crime suppression activities deter terrorism.

Simply stated, risk is the possibility of damage happening to an organization.[16] The three steps to performing a risk analysis are identifying the risk, determining the impact of threats, and balancing the impact of threats with safeguards.[17] The threat to rail transport is concerning despite the fact that no significant act of terrorism against the rail system has occurred in the United States, although domestic law enforcement authorities have thwarted planned attacks, such as those directed against the New York City subway system. Modern high-density passenger rail transportation has one overarching intention: to achieve the rapid movement of high volumes of passengers through an open architecture. Metropolitan transportation systems, by their very nature, pass through and under some of the most densely populated metropolitan landscapes in the world. Consequently, a relatively low level of sophistication is required to stage an attack against one of these systems. The possibility of a large number of casualties and significant disruptions makes the time and planning needed to stage an attack worth the effort. Attacks on underground networks cause alarm and distress among the commuter population, network paralysis, lengthy disruptions, and economic loss.

## D. SIGNIFICANT ATTACKS

There are a number of specific attacks that reinforce the consensus that passenger rail systems are and will continue to be prime targets of terrorisms in the future. The summary that follows is in chronological order of occurrence. Due to the deadly results of these incidents, they stand as reminders of the importance associated with this

---

[15] International Atomic Energy Agency, *Safety Assessments for Facilities and Activities* (Vienna: International Atomic Energy Commission, 2009), 35.

[16] Ibid., 13.

[17] Milagros N. Kennett, Eric Letvin, Michael Chipley, and Terrance Ryan, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings* (Washington, DC: Federal Emergency Management Agency, 2005), 90.

problem. An analysis of the circumstances surrounding these events, such as the existing conditions, the tactics and techniques employed, and the gaps exploited, has relevance in improving security resource decisions that reduce risk exposure to terrorist attacks.[18] In conducting risk assessments, Jeremey Plant advises, "it is important to take into account relevant data from international examples of acts of terror that have been directed at rail systems."[19]

The first significant attack occurred in March 1995 when the Aum Shinrikyo religious cult assaulted the Teito Rapid Transit Authority system. This event is most notable chemical attack ever to occur in mass transit. Cult members released sarin gas, a nerve agent, during the morning rush hour on five trains that were operating on three different lines. They carried the devices into the system in plastic bags. The bags were dropped inside the trains and pierced to allow the liquid to escape. At total of 16 stations were contaminated in less than 10 minutes. As a result, hundreds of passengers fell ill, 12 killed, and more than 5,500 injured. Additionally, 130 first responders succumbed during rescue efforts, not knowing that it was a chemical attack. Conformity is the convention in Japan's social system. Consequently, the authorities were surprised that such an incident occurred.[20] What saved more people from being injured or killed was the inferior quality of the chemical agent and the dispersal mechanism used by the terrorists.[21]

Islamic terrorists conducted two successful attacks in July and October of 1995, killing a total of eight and wounding more than 200. Improvised explosive devices (IEDs) were placed inside stations and detonated during rush hour. At the time, rail security in Paris was ad hoc. There was little coordination or communication between security

---

[18] John Markey, *Terrorism Risk for Public Transportation Systems*, NATO Science and Peace for Security Series, Vol. 54 (Amsterdam: IOS Press, 2009): 117.

[19] Plant and Young, *Securing and Protecting America's Railroad System*, 54.

[20] Anastasia Loukaitou-Sideris and Brian Taylor, "Rail Transit Security in an International Context, Lessons from Four Cities," *Urban Affairs Review* 41 no. 6 (2006): 7.

[21] Lisa Staes, Amber Reep, and Rajesh Chaudhary, *Identification of Cost-Effective Methods to Improve Security at Transit Operating/Maintenance Facilities and Passenger Stations* (Washington DC: U.S. Department of Transportation, Federal Transit Administration, 2006), 43.

services to better protect riders and assets.[22] Moreover, the industry had no systemic approach to security in addressing vulnerabilities.

In March 2004, a group of terrorists placed 13 IEDs on four separate passenger trains. Ten of the devices detonated within 30 minutes of each other during the morning rush hour resulting in 191 killed and 1741 wounded. Some of the IEDs exploded as trains were arriving in stations, which increased the number of casualties. Others detonated near doorways, where passengers congregate, which also caused additional casualties.[23] Not only were rail cars severely damaged, but tracks and a station suffered significant damage as well. The rail system had no passenger security awareness program in place. In addition, the devices were hidden in baggage that was left unattended on the trains. If the system had a security awareness campaign alerting passengers to notify train crew of suspicious items, the attack could have been disrupted.

Suicide bombers carried out a successful coordinated attack against the London mass transit system in July 2005. Three suicide bombings occurred on trains and a fourth exploded on municipal bus during rush hour. The attack against the bus resulted from one of the individuals missing his train. Being flexible, he chose a bus as an alternate target. The overall result was 52 killed and approximately 700 injured. All four bombers were killed during this attack.[24] MI-5, the country's national intelligence agency, failed to follow-up on potential leads identifying the perpetrators to known terrorists. Also, local law enforcement authorities did not follow-up on information regarding suspicious activity linked to one of the perpetrators.[25]

In July 2006, terrorists placed IEDs in the first car on each of seven different commuter railway trains in Mumbai, India. The explosions, which occurred within 15 minutes of each other, caused 190 deaths and wounded 625.[26] The devices were

---

[22] Ibid., 5.

[23] Jenkins and Butterworth, *Analysis of Terrorist Attacks*, 1.

[24] Stephen M. Lord, *Passenger Rail Security, Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives* (Washington DC: General Accountability Office, 2012), 48.

[25] Markey, *Terrorism Risk*, 10.

[26] Lord, *Passenger Rail Security*, 48.

constructed in pressure cooker containment vessels.[27] Given the frequency of attacks in India, there was a striking lack of security, such as emergency response, crisis management planning, and coordination. This left gaps in the system, which were exploited by terrorists.[28]

Suicide bombers struck the Moscow Metro System during rush hour, in March 2010, by planting IED's on board trains, which resulted in 40 dead and 58 injured. The initial explosion occurred on a train arrived at the Lubyanka station. The second blast occurred at passengers boarded at the Park Kultury station. Chechen separatists were credited with the attacks.[29] The Moscow bombers used suicide belts containing screws and pieces of iron rods to make shrapnel. The precise timing indicates the terrorists themselves detonated their own devices.

In March 2016, a suicide bomb detonated on a train at the Maelbeek Station in the Brussels Transit System. The explosion occurred as the train departed the station and killed 16 passengers. The attack site was near a section of the city that housed European Union institutions, including European Union headquarters and the Council of the European Union. Details associated with this attack indicate that the terrorists were most likely familiar with the targets, conducted preoperational surveillance, and did some level of planning prior to the attack.[30] The IEDs were constructed with triacetone triperoxide. This compound is made from chemicals that are readily available commercially through supply stores and on-line companies.

All of the events, described above, exposed security gaps on a particular system. A key similarity in these incidents was that the attackers were radicalized individuals.[31] Differences include the composition of the IEDs. In some cases, it was mining

---

[27] Markey, *Terrorism Risk*, 10.

[28] Lord, *Passenger Rail Security*, 28.

[29] Cathleen A. Berrick and Jayetta Hecker, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* (Washington, DC: Diane Publishing, 2006), 14.

[30] U.S. Department of Homeland Security, *Tactics, Techniques, and Procedures Used in the 22 March 2016 Brussels Attacks* (Washington DC: Office of Intelligence and Analysis, 2016), 3.

[31] Michael Jones, "Understanding the Terrorist Threat to Underground Rail Networks—Part 1," *Jane's Terrorism & Security Monitor* (summer, 1995): 2.

explosives, in others triacetone triperoxide or in the March 2010 bombing, military grade nitrosamine. Another contrast was that some attacks were performed by suicide bombers, while others planted devices allowing the perpetrators to escape.

## E. RESEARCH DESIGN/HYPOTHESIS

Rail systems use a variety of risk assessment methods. Large operators have the resources to develop complex processes, but smaller operators do not have the same resources. They are subject to constraints, such as budgetary support, which restricts their ability to employ the same risk assessment programs that larger operators utilize.

The research underlying this thesis incorporates the guiding principles of the risk assessment methodology. Examining the threat environment and factors associated with defense against malicious actors will result in a better understanding of the assessment options available to defend against threats. The proposed model will useful to rail system executives and security staff personnel. Furthermore, it will encourage those responsible for passenger rail security to balance the effectiveness of counter measures and resource implementation, including operational issues and costs.

# II. LITERATURE REVIEW

This literature review provides an overview of areas that impact strategies used to safeguard passenger rail assets from terrorism. Although two of the most significant rail terrorism events, the Madrid and London bombings, took place in 2004 and 2005, respectively, the United States rail industry had earlier expressed concerns about security in the aftermath of the World Trade Center attacks in 2001.[32] Given recent international attacks, the efforts to strengthen passenger rail security are important today as they were 15 years ago, immediately after 9–11.

Coming from academia and scholarly research, literature on rail security is organized into the following subjects: environment/landscape, system modeling, ownership, governance/regulations, policies, and examples. Other literature falls into one of following source types: reports from governmental organizations, such as the Government Accountability Office and the Congressional Research Service; rail industry trade groups, such as the Association of American Railroads and the American Public Transportation Association; and non-profit groups, such as the RAND Corporation and the Mineta Transportation Institute.

## A. ENVIRONMENT/LANDSCAPE

The passenger rail component of the transportation sector is vital to the U.S. economy.[33] In addition, the public benefits from efficient, rapid transit for a host of needs that includes commuting to work, attending school, or traveling for leisure activities. Loss of the passenger rail network would further overburden the highway infrastructure in our country's biggest cities as well as constrict business and government activities. More than 300,000 workers are employed in this industry to ensure reliable service, adding further economic benefits.[34]

---

[32] Daniel Morgan and H. Abramson, *Improving Surface Transportation Security Through Research and Development* (Washington DC: National Academy Press, 2000), 19.

[33] Jeremy M. Wilson, Brian A. Jackson, and Mel Eisman, *Securing America's Passenger Rail Systems* (Santa Monica, CA: RAND Corporation, 2007), 16.

[34] Boyd and Sullivan, *Emergency Preparedness*, 12.

Passenger rail has played a significant role in the development of the American landscape. According to Eric Monkkonen in *America Becomes Urban: The Development of U.S. Cities and Towns 1780–1980*,

> Transportation technologies such as trains shaped how cities are today. The influence of government, through subsidies for emerging technologies such as trains, had a profound effect on the relationship between transportation and urban geography. Local action created the environment that fostered the new technologies and their subsequent adoptions. Railroad rights-of-way were developed before any technology could be invested in and perfected. These changes occurred at the local level, bringing the role of government rather than that of technology, to the forefront.[35]

The passenger rail sector is experiencing a revival. In 2013, there were more than 4.8 billion rail trips in the United States.[36] More than 11.3 million passengers in 35 metropolitan areas utilize rail transportation daily, which is the highest level of ridership since 1957.[37] The New York City area by itself accounts for 40 percent of the trips for the entire country.[38] Annual subway ridership on the New York City subway system has increased by more than 60 percent from 1.028 billion riders in 1990 to 1.7 billion in 2015.[39]

There are approximately 100 passenger rail systems in the United States. They fall into four categories: heavy rail, service exclusive tracks with the capacity to handle a heavy volume of traffic; light rail, single rail vehicles or short trains in segregated rights-of-way with grade crossings or in shared-use roadways; commuter rail, regional service into metropolitan areas from adjacent suburbs; and intercity rail, inter-state and inter-

---

[35] Eric H. Monkkonen, *America Becomes Urban: The Development of U.S. Cities and Towns 1780–1980* (Berkeley: University of California Press, 1988), 158.

[36] American Public Transportation Association, "Quarterly and Annual Totals by Mode, 1990–present," www.apta.co m/resources/statistics/Pages/ridershipreport.aspx, accessed July 23, 2014.

[37] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, iii.

[38] R. William Johnstone, *Protecting Transportation: Implementing Security Policies and Programs* (Waltham, MA: Butterworth-Heineman, 2015), 78.

[39] Metropolitan Transportation Authority, "New York City Transit Information," accessed May 28, 2016, http://web.mta.info/mta/network.htm.

regional service.[40] Greater numbers of Americans are settling in urban areas, which puts additional stress on passenger rail transportation. According to a 2015 report by the U.S. Census, 62.7 percent of the population resides in or around cities.[41] As the population continues to move toward urban areas, cities develop into a patchwork of urban nodes. Centric areas with pockets of urbanization become connected by mass transit, such as light rail systems. Examples of recent new system starts in growing urban areas include New Jersey Transit's expansion along the Hudson River in Newark and Hoboken, Atlanta's Beltline, and the Redline in Baltimore.[42]

Recent worldwide attacks show that terrorists are intent on inflicting damage to passenger rail assets. According to reports from the Transportation Security Administration's Office of Intelligence, the following characteristics make passenger rail systems an attractive target for terrorists

- The passenger rail infrastructure is open. There are multiple points of access and egress. There are no substantial barriers that restrict large numbers of people from moving about quickly and easily.
- Interconnectivity between carriers has created hubs resulting in the ability to enter into a network at multiple locations.
- Operations personnel cannot completely monitor who enters or leaves a system.
- Locations in metropolitan areas include tourist destinations with dense crowds, which provide opportunities for mass casualties, economic damage, and disruption.
- Large numbers of riders make screening, similar to the level that travelers experience in aviation, impossible in passenger rail.[43]

---

[40] American Public Transportation Association, *2013 Public Transportation Fact Book*, 64th ed. (Washington, DC: American Public Transportation Association, 2013), www.apta.com/resources/statistics/Documents/FactBook/2013-APTA- Fact-Book.pdf.

[41] Darryl T. Cohen, *Population Trends in Incorporated Places 2000–2013* (Washington DC: U.S. Census Bureau, 2015), 1.

[42] Yonah Freemark, "Passenger Rail Projects under Way," The Transport Politic, accessed September 18, 2016, http://www.thetransportpolitic.com/under-consideration/planned-light-rail-systems/.

[43] U.S. Department of Homeland Security, *Strategic Sector Assessment: Potential Terrorism Threat to U.S. Mass Transit Systems* (Washington DC: Office of Intelligence and Analysis, 2006), 8.

The following breakdown provides insight into the tactics that have been used in attacks between 1920 and 2007 (see Table 1).[44]

Table 1. Common Methods for Passenger Rail Attacks[45]

| Tactic | Number | Percentage |
|---|---|---|
| Armed attack | 55 | 6 |
| Arson | 29 | 3 |
| Barricade or hostage | 2 | 0 |
| Bombing | 708 | 80 |
| Hijacking | 2 | 0 |
| Kidnapping | 3 | 0 |
| Sabotage | 49 | 6 |
| Unconventional attack | 24 | 3 |
| Unknown | 9 | 1 |
| Logistics activity (non-attack) | 5 | 1 |
| **Total** | 886 | 100 |

In *Securing America's Rail Systems*, Wilson, Jackson, and Eisman stress that when developing security defenses, system security personnel must consider the types of attacks that at are preferred by terrorists. These include bombings, armed attacks, sabotage, and unconventional attacks. Some of the more common attacks are described below.

The frequent use of explosive devices in the past makes it likely that bombings will be the preferred method in future attacks. Timed IEDs allow terrorists to conduct

[44] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, 32.

[45] Adapted from Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*.

attacks without losing personnel. Suicide operations provide another strategy for groups to increase effectiveness because an assailant can react to conditions and maximize the effect of the attack as it unfolds. Terrorists have the option to focus on single devices that target one segment of a rail system, or increase the severity by planting multiple devices.

Armed attacks have recently increased. Firearms can be employed in singular attacks or in complex assaults featuring multiple shooters. Attackers use sabotage to disrupt operations and cause fatalities. The advantage is that weapons are not required. Insider threats are relevant to this attack mode.

Although terrorist use of unconventional weapons has been rare in the past, the 1995 sarin gas attack in the Tokyo, demonstrated that chemical, biological, and radiological devices can be successfully deployed.[46] The incident showed how crowds of travelers in confined spaces enhanced the device's effectiveness and increased the potential impact of these types of weapons. Even if the potential of these types of attack occurring is low the consequences are so high that systems must dedicate resources to protecting and recovering from the use these weapons.[47]

Wilson, Jackson, and Eisman also identify areas of the system that provide the environment necessary to maximize the attacker's expenditure of resources (see Table 2).[48]

[46] Brian Jackson, John Baker and Peter Chalk, *Aptitude for Destruction*, Organizational Learning by Terrorist Groups and Its Implications for Combating Terrorism, Vol. 1 (Santa Monica, RAND Corporation, 2007), 3.

[47] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, 15.

[48] Ibid., 42.

Table 2. Common Rail System Areas[49]

| Area Type | Definition |
|---|---|
| Perimeter areas | Access routes, pathways, elevated infrastructure, tunnel entrances, underground infrastructure, tracks and railroad crossings |
| Exterior areas | Station interiors from entrances to ticketed-passenger entry |
| Interior areas | Station interiors beyond ticketed-passenger entry points to train platforms |
| Restricted areas | Rail-operation, maintenance, operation control center, power-generation plant |
| Assets | Trains |

Transportation systems are susceptible to damage in ways that are overlooked in day-to-day activities. In addition, terrorists are actively seeking to capitalize on vulnerabilities that lie beyond the conventional perceptions of order. Because of this, the passenger rail industry has to develop a broader-based understanding of the threats so that transit systems can protect the public from terrorism.

## B. SYSTEM MODELING

Passenger railroads are large, complex networks with many segments working in unison to efficiently and safely transport people. A diverse group of operators controls these networks. On the surface, companies may appear to operate in the same fashion. There are similarities, particularly in regulated activities, such as operational policies and procedures because of decades of experience that have influenced the industry to adopt practices, which today have become the standard way of conducting business. However, there are differences in other disciplines, such as security policies, which have resulted in

[49] Adapted from Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*.

a variety of approaches from one system to another. Companies have latitude on how to perform these activities.

The physics, protocols, standard operating procedures (SOP), and practices, which support the framework in which rail transportation operates, are integral to the rail system domain. Protocols or SOPs are the system of rules that govern the operation of passenger railroads, and variations are based on the type of system that a company runs. Commuter rail protocols differ from those of heavy rail/subways and light rail. In addition, protocols can be voluntary or mandatory in nature. Moreover, government oversight on the federal and state levels have major influence on rail operations. William Waugh noted in "Securing Mass Transit: A Challenge for Homeland Security," that trade organizations, such the American Public Transportation Association (APTA), use best practices and peer advisory groups to bring all operators into alignment with recognized safety and security practices.[50] Recommendations from industry partners are adopted through voluntary compliance. Most government activities fall in the realm of regulations, which are tied to mandatory compliance.

The purpose of passenger rail is to transport people efficiently and safely. Efficiency involves moving large numbers of people in a timely fashion according to a schedule. Safety means transporting passengers to their destination without mishap. Safety and security are interrelated as both strive to ensure that passengers are not injured. Although the safety and security culture are different, the intended outcome is the same.

The typical passenger rail operates is in a metropolitan area and the development of a railroad relates to the growth of the locality that it serves.[51] An example of this phenomenon is the city of Boston, which developed into a thriving metropolis because of its extensive rail system. Passenger railroads have certain characteristics that developed over time, and each feature has a function and adds value to overall efficiency. For

---

[50] William Waugh, "Securing Mass Transit: A Challenge for Homeland Security," *Review of Policy Research* 21, no. 3 (2004): 311.

[51] John Armstrong, *The Railroad: What It is, What It Does* (Omaha, NE: Simmons-Boardman Books Inc., 1998), 4.

example, there are elevated and below-ground stations and hub stations that provide riders with transfer points. In addition, there are support facilities such as power distribution, command and control, and storage and repair yards. Various lines serve specific geographical areas, which may reach beyond the municipal boundaries of a city to suburban regions. Additionally, there is connecting service to other transportation systems, such as bus lines, airports, ferries, and other passenger rail systems, such as inter-city rail. Internal features include perimeter and station surveillance systems, a uniformed security presence, and an automated car locator system, which monitors train flow.

Trains must overcome resistance to move. Rolling resistance corresponds to wheels on the rail. This friction is energy that is not recoverable when expended. Grade resistance results from the energy that a train uses to lift vertically. That energy is recaptured when the train travels down the grade to a lower level.[52]

The forces of physics in play are quite impressive as a system operates. A locomotive and four passenger cars weigh approximately 100 tons. Engineering plays a large part in overcoming friction. The force of the wheel flanges, which are directed down upon the rail components on a 260-foot section of track includes 11 tons of steel, 3 tons of rail fasteners, 16 tons of track ties, and 130 tons of rock ballast, determine the design of the system.[53] Increases and decreases in direction can occur on the vertical axis or on the horizontal plane. The curvature counters centrifugal force, which tends to push trains away from the inside of a turn. The concept of super-elevation was adopted to build up of the outer rail to mitigate the influence of centrifugal force, eliminating the possibility of a train derailing and toppling off the outside rail as it attempts to succumb to the forces in play.

Two factors that give a train the ability to move are traction and horsepower. Traction is the force needed to turn a train's wheels and move it forward.[54] A train

---

[52] Joseph Flaus, *Risk Analysis: Socio-Technical and Industrial Systems* (Hoboken, NJ: John Wiley and Sons, 2013), 29.

[53] Ibid., 19.

[54] Ibid., 55.

generates this pull by gripping the rail with its driving wheels. The train's weight must be several times the tractive force that needs to be developed to move it, and a high level of adhesion results in more efficient operation. Horsepower is the measure of the rate of doing work. The weight of a train at a particular speed traversing a given gradient determines the power required to move a train. There are many variables on the operation side of the system that must be considered when passenger rail cars operate.

Furthermore, there are distinct components in a passenger rail system. The industry operates under a structure that separates the responsibility for activities into departments such as operations, which ensures the serviceability of cars; facilities, which maintains stations; power distribution, which supports connectivity, maintenance of way for track integrity; and signaling, which monitors communications.[55]

The contributions of some components are highly visible to the public, such as the physical condition of stations and the operation of trains. The accomplishments of others, such as signals, are largely hidden and not fully appreciated by the ridership. They function in unison to accomplish the end result of passenger transport. All segments, whether stations, trains or tracks, are at risk from one type of attack or another. The difference is that each component has features that make it susceptible to a particular attack method. An understanding of the characteristics of a rail system reveals some of these vulnerabilities.

A primary component of the railroad infrastructure is track. It consists of rails, fasteners, crossties, and ballast. There are more than 7,000 miles of track in the U.S. passenger rail system.[56] Some systems operate on exclusive tracks, where passenger trains are the only traffic operating on a particular section of rail. On others, a freight rail company may own the tracks and share use with a passenger system. Track may seem substantial in terms of composition, but in comparison to the loads it must bear, it is only a fraction of the weight that it must support. Tracks are laid out in a specific configuration on purpose. All characteristics, including tangents, curves, switches, and

[55] Armstrong, *The Railroad*, 251.

[56] Staes, Reep, and Chaudhary, *Identification of Cost-Effective Methods.*

grading are in place for a reason related to either topography or cost. The main focus in rail security today—trains and stations—may have the effect of directing attention away from track security.[57] Intentional damage to tracks will shut down or degrade the operation of a railroad, such as incidents in India and Pakistan in recent years when tracks were targeted by IEDs.[58] Policymakers need to consider track security in any strategy for protecting a system against attacks.

The signaling and communication systems of a railroad are synonymous with the nervous system of a human being. The railroad is a "single degree of freedom" transportation mode.[59] Trains can only go back and forth along the tracks. Restricted to only one degree of freedom, attaining high capacity and safety depends on a control system that keeps trains in proper relation to each other. The purpose of signaling is to increase the efficiency and capacity of a line to handle traffic. The compromise of a signaling system, whether due to failure of equipment, such as a broken rail, a faulty wire connection, or an act of terrorism, could result in a shutdown. Communication systems use centralized digital computation for operational and business aspects, such as tracking the location of trains in the network. Since railroads operate over long distances, management information services have become vital, as they have in most other industries. Remote monitoring and control via supervisory control and data acquisition, while highly efficient, exposes railroads to the potential network attacks. This information technology (IT) infrastructure is responsible for controlling the movement and monitoring of transportation equipment.[60]

Rail cars or trains are one of the most tangible facets patrons see of a passenger rail line. System capacity is dependent on the configuration of cars, and the number of doors on a train governs the rate at which passengers can get on and off. A system that

---

[57] Ben Lerner, "Losing Track on Rail Security," *Homeland Security Today*, April 25, 2016, http://www.hstoday.us/columns/guest-commentaries/blog/losing-track-on-rail-security/fff77b506f8b611b018f4234254a5180.html.

[58] U.S. Department of Homeland Security, *Tactics, Techniques, and Procedures*, 8.

[59] Armstrong, *The Railroad*, 125.

[60] American Public Transportation Association, *Cyber Considerations for Public Transit APTA SS-ECS-RP-001-14* (Washington DC: Enterprise Security Working Group, 2004), 1.

operates eight 75-foot cars at rush hour capacity with 90-second headway could hypothetically exceed the capacity of a 20-lane expressway full of single occupant vehicles.[61]

Heavy rail cars and commuter cars have different manufacturing specifications, and the speed at which these trains operate is the determining factor for survivability or crash worthiness in accidents. In addition, many of the advances in train design revolve around crime prevention strategies. Graffiti resistant surfaces, increased visibility through the incorporation of glass, and intercom systems have resulted in a safer environment for riders. These advances have the ancillary benefit of deterring terrorism as well. The interior of cars has been designed to eliminate shrapnel-producing interior fixtures and voids or areas where IEDs can be hidden.

A measure of efficiency in rail cars is ridership capacity. Accommodating more passengers in a rail car translates into more revenue for the operator. Unfortunately, congested cars provide an opportunity for terrorism, particularly those using explosive devices. Confined spaces magnify blast effects, and train cars are efficient containment vessels. Of all the components of a rail system, trains are one of the most at risk. Furthermore, the majority of terrorist attacks have targeted trains and underground networks.[62]

Stations are another major part of a rail system. Their architectural features, such as multiple entrances and exits, maximize movement. Often there are multimodal connections with other transit systems and buses to encourage patronage. Each facility, whether it is an aboveground or an underground station, has unique security challenges. Underground stations pose concerns in regard to the integrity and ability to sustain damage and resist collapse. Since stations consistently draw crowds, commercial development is incorporated into facilities. These characteristics make screening of

---

[61] Armstrong, *The Railroad*, 243.

[62] Tony Pattison, "The Daegu Subway Tragedy: Was it Avoidable?" *Jane's Terrorism and Security Monitor*, July 27, 2005, 3.

passengers in the traditional sense almost impossible to accomplish.[63] In *Hard Won Lessons: Transit Security*, Charles Sham emphasizes that "Incorporation of certain elements, such as reinforced construction materials, can reduce the damage from an explosion. Likewise, injuries from a terrorist attack can be mitigated when physical considerations are included in the design of features such as entrances and exits."[64]

Railroad personnel strive to ensure that all of the components of the system function properly. The majority of a rail system's employees, up to 85 percent, are in the operations division.[65] These people run the railroad. There are administrative positions such as dispatchers, and management, as opposed to field positions, such as engineers, conductors, and station agents. Railroad operators are encouraging all employees to serve as additional eyes and ears, in an effort to increase domain awareness. The goal is to detect suspicious activities before an attack occurs. In a 2005 report issued by DHS entitled, *How Security Personnel, Transit Employees, and Passengers Disrupted Attacks against Mass Transportation Worldwide*, the following observations were noted

> Forty Four percent of attempted IED attacks, 32 incidents worldwide, between 2004 and 2010, failed as a result of observations by employees or security personnel. Reporting suspicious persons or packages is a core responsibility of employees because workers have superior domain awareness of the rail system. The majority of employees know the trains, tunnels, and passengers better than anyone else. Information gathering should also involve the millions of passengers who commute each day. By utilizing the public as a 'detection' system, an agency can exponentially increase the chance of detecting suspicious persons and packages.[66]

Depending on the configuration, there may or may not be power facilities on a system. Electricity is the source of power on the majority of the country's networks, and distribution occurs through either third rail or overhead catenary wires. Rail power

---

[63] U.S. Department of Homeland Security, *Characteristics and Common Vulnerabilities: Railroad Passenger Stations* (Washington DC: Protective Security Division, 2005), 14.

[64] Charles Sahm, *Hard Won Lessons: Transit Security* (New York: Manhattan Institute for Policy Research, 2006), 17.

[65] Armstrong, *The Railroad*, 269.

[66] U.S. Department of Homeland Security, *How Security Personnel, Transit Employees, and Passengers Disrupted IED Attacks against Mass Transportation Worldwide, 2004-2010* (Washington DC: Office of Intelligence, 2011), 3.

facilities do not produce electricity; rather, they transfer voltage from a local generation system, such as a municipal power company, to the network where rail power plants convert it from alternating current to direct current prior to distribution. On some systems, diesel equipment provides propulsion. Rail systems are vulnerable to loss of power, which could occur from any sort of hazard, such as weather or equipment malfunction, and not just deliberate actions such as terrorism.

## C. OWNERSHIP

Railroads are owned by corporations that are usually run by a board of directors and headed by a chief executive officer responsible for long-range plans and practices. State and local governments own the majority of mass transit and passenger rail systems in the United States.[67] While the federal government supports construction with grant funding, it owns little, if any, of the infrastructure. There are hybrid systems in which a private entity is contracted to operate and maintain all or part of a system on behalf of the government. Certain parts of a system, such as tracks, trains, and stations may be public assets while others may be owned by a private corporation. For instance, some trains operate on territory that the government does not own, and some of the infrastructure may be the private property of a freight railroad.

A group of executives who run a passenger rail system, such as New York City Transit (NYCT), is accountable to elected officials. In addition to revenue from fares, public funds are dedicated to operational costs, so the public owns the passenger rail system. State or local governments are obligated to handle emergencies on a rail system that runs through their jurisdiction. The primary responsibility for security rests with the passenger rail system operators even though all levels of government are involved in this activity.[68]

---

[67] Cathleen A. Berrick, *Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs* (Washington D.C: Diane Publishing, 2006), 17.

[68] Berrick and Hecker, *Passenger Rail Security*, 18.

## D. GOVERNANCE/REGULATIONS

The federal government has the lead on counterterrorism efforts, both public and private, for passenger rail. In *Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*, Cathleen Berrick clarifies that the federal government's primary role is "to promote the use of existing technologies, research and development activities, and deployment of new approaches to mitigating the nation's vulnerabilities."[69] In addition, the federal government also sets standards for performance and interoperability. To accomplish this, the federal government requires cooperation with other entities including state and local governments, industry, organizations, and other institutions. In *Securing America's Railroad Systems*, Plant and Young agreed that

> Security oversight in rail, since 9–11, has taken a different path than in other transportation modes. Private sector action has filled part of the vacuum that existed for several years as the federal executive put higher priorities on other aspects of homeland security and the war on terror. This imbalance between public policy and private sector action is being partially addressed as stronger network collaboration is emerging between the Transportation Security Administration (TSA) and the rail industry.[70]

It may require regulatory action to convince the rail industry that investing in systems to reduce vulnerabilities or to develop counterterrorism technologies is in their best interests, despite the reluctance to dedicate profits for non-mandated security enhancements.[71]

Several agencies provide regulatory oversight for the passenger rail industry. There are overlaps, and duplication of effort is apparent in some of the programs. The Aviation and Transportation Security Act of 2001 identified the Transportation Security Administration (TSA) as "the governmental entity responsible for security in all modes of transportation including passenger rail."[72] The TSA sets national priorities, develops

---

[69] National Research Council, *Deterrence, Protection, and Preparation*, 28.

[70] Plant and Young, *Securing America's Railroad Systems*, 61.

[71] National Research Council, *Deterrence, Protection, and Preparation*, 90.

[72] Aviation and Transportation Security Act of 2001, Public L. No. 107-71 (2001).

strategies, and outlines plans for addressing security threats. Even though the TSA has statutory authority, it has issued only a handful of minor regulations. Instead, the agency has chosen to work in partnership with the passenger rail industry and promulgates voluntary action items. In addition, the Office of Security Police and Industry Engagement has developed policies and plans to reduce the risk of catastrophic terrorist attacks. The Surface Transportation Security Inspection Program implements programs, conducts assessments, inspections and other activities in mass transit and passenger rail, and the Office of Intelligence collects and analyzes threat information related to the rail transportation network and disseminates data to industry regarding potential threats.

The National Protection and Programs Directorate, within the Office of Domestic Preparedness, is another agency in DHS involved with rail security. This agency, established by *Homeland Security Presidential Directive 7*, coordinates the domestic effort to reduce risk for critical infrastructure, including assistance with response and recovery capabilities in cases of attacks, natural disasters, and other emergencies.[73] The goal of these governmental agencies is to make systems resilient and secure.

Another component of DHS that plays a role in fortifying security in the U.S. rail system is FEMA. Although it has no regulatory status in security matters, it controls a key resource, funding, specifically the Transportation Security Grant Program (TSGP).[74] The millions of dollars dedicated for security enhancements through the TSGP provide much needed financial support to strengthen the security posture of passenger rail systems. Between 2002 and 2016, the TSGP awarded more than $2.4 billion to 60 rail systems.[75] Proponents in favor of federal funding for security improvements argue that foreign terrorists pose the greatest threat. This means the federal government must take responsibility for supplemental funding in its role of providing for the national defense.[76]

---

[73] U.S. Department of Homeland Security, *NPPD at a Glance* (Washington DC: U.S. Department of Homeland Security, 2014), https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf.

[74] Berrick and Hecker, *Passenger Rail Security*, 8.

[75] Bart Alias, *Transportation Security: Issues for the 114th Congress* (CRS Report No. RL33512) (Washington DC: Congressional Research Service, 2016), 21.

[76] David Randall Peterman, *Passenger Rail Security: Overview of Issues* (CRS Report No. RL32625) (Washington DC: Congressional Research Service, 2005), 8.

According to estimates from the Federal Transit Administration (FTA), rail entities need to increase capital expenditures anywhere from $3 billion to $8 billion annually to upgrade the security infrastructure.[77]

Government entities, aside from DHS, play a role in transportation security matters. The U.S. DOT modal administrations provide support in the federal government's efforts to improve rail security. The Federal Railroad Administration (FRA) focuses on safety regulations dealing with areas such as equipment, employee qualifications and transportation of hazardous materials. If tracks connect to the national rail system, meaning a train is capable of moving from one system to another, the operation falls under the oversight of the FRA, which has additional security regulations. This pertains to commuter and intercity rail systems. The FRA provides technical assistance in matters related to emergency management, infrastructure, and risk management.[78]

The FTA similarly engages in safety and security activities such as research, development, and pilot projects. The agency also promotes security through grant funding and provides assistance for the development of new systems and the improvement of existing ones.[79] However, the FTA's jurisdiction differs from the FRA. If the tracks of an operation are independent of the national rail system, which prevents trains from switching from one system to another, then the FTA retains oversight.

Trade associations, such as the APTA, also exert influence on the passenger rail sector. APTA represents the public authorities as well as private companies that design, construct, supply, and operate systems.[80] Furthermore, APTA has been active in supporting voluntary safety management, which includes audits and publication of industry best practices.[81]

---

[77] Ibid., 8.

[78] Berrick, *Key Actions*, 40.

[79] Ibid.

[80] American Public Transportation Association, *Identifying Suspicious Behavior in Mass Transit* (APTA SS-SRM-RP-009-09) (Washington DC: Enterprise Security Working Group, 2009), 126.

[81] Armstrong et al., *Securing America's Passenger Rails*, 4.

## E. POLICIES

Securing transit systems presents political problems. In *Securing Mass Transit: A Challenge for Homeland Security*, Waugh notes that systems that run across multiple jurisdictions rely upon the financial support of more than one governing body. Safeguarding infrastructure and securing financing for improvements requires coordination among many levels of government, as well as private entities and federal agencies.[82]

In *Securing America's Passenger Rails*, Armstrong, Bland, and Cox explain there are two systems when it comes to state and local interactions, Dillon's Rule and Home Rule. Dillon's Rule confines local authority to powers that a state has delegated. Conversely, Home Rule defaults to local authority unless the state claims jurisdiction. When Dillon's Rule applies, leaner interagency relationships result in simpler incentives. Home Rule involves more comprehensive incentives to appeal to all entities involved. The federal government can exert leverage on heavily subsidized sectors, such as mass transit. In *Securing America's Passenger Rails*, Armstrong, Bland, and Cox argue that the federal government has a responsibility to protect the homeland, but it has limited options as to how to require local governments to implement security measures. Even if incentives are tied to grant funding, many states may not want to abide by the stipulations attached to grants.[83]

Armstrong, Bland, and Cox go on further to explain that the principle of delegation of authority, which empowers government agencies to pursue their mission of addressing security issues, is divided into three models: the agency-centered approach, the networking approach, and the balanced approach.[84]

The agency-centered approach gives a governmental entity general authority to plan and implement public programs. Accountability derives from a government agency's ability to find ways to achieve performance standards either specified in law or

---

[82] Waugh, "Securing Mass Transit," 311.

[83] Armstrong et al., *Securing America's Passenger Rails*, 42.

[84] Ibid., 50.

developed in the course of implementing the program. The agency is also able to develop critical relationships with organizations inside and outside government. The ends expressed, in performance based terms, are the basis of accountability and allow executives to find the most effective way to reach goals.

The networking approach assumes that traditional top-down bureaucracies are inadequate to deal with emerging problems or with ill-defined boundaries or characteristics. The goal of management is to develop trust among the participants, facilitate the sharing of resources and information, and respond intelligently to changing conditions and problems. Agencies empowered to create network approaches to problems are tasked with creating opportunities to share information and work with other public and private organizations with which they share some common goal.

The balanced approach incorporates elements of both the agency-centered and network models. The development of legislation on rail security will allow all interested and affected parties a chance to influence the policy formation. Memoranda of understanding between federal agencies engaged in rail security oversight (e.g., DOT and DHS) should plainly spell out the responsibilities of each agency for purposes of accountability and effectiveness. The balanced approach must be flexible enough that a network of interested parties—the private rail industry and public sector rail authorities—continues to provide needed input and effort to a coordinated and cooperative approach to rail security.[85]

The U.S. government's current posture, considering the minimal scope of regulations, is in line with the balanced approach. The federal government, particularly the TSA, has promulgated regulations. At the same time, the TSA has partnered with industry and engaged in a collaborative effort to ensure compliance with security best practices to safeguard the passenger rail sector.

According to APTA, the majority of passenger rail agencies are facing deficits, and no U.S. system can cover expenses through revenue.[86] State and local governments

[85] Plant and Young, *Securing and Protecting*, 37.

[86] Berrick, *Key Actions*, 51.

provide 21and 22 percent of expenses while the federal government adds four percent.[87] Fares contribute 36 percent of expenses. According to testimony given by Peter Guerrero, Director Physical Infrastructure Issues, before the U.S. Senate Subcommittee on Housing and Transportation, the federal government supplements capital expenses by 47 percent and provides most of the funding for building and maintaining these systems.[88] Operating expenses are provided through state and local funding. Since security enhancements are operating expenses, the burden of paying for them falls primarily upon the taxpayers and riders.[89] In *Securing Mass Transit*, Waugh explains,

> Federal regulations prohibit large systems (serving populations over 200,000) from using capital funds for operating expenses like security, so operators face a monumental task in terms of securing stations and routes. In short, transit systems are hard-pressed to find internal funding and are therefore dependent upon the federal grants to implement security improvements. Consequently, in the absence of federal dollars, much of the investment in security has been voluntary and very limited.[90]

Establishing equity in security funding for rail as compared to other modes, such as the aviation, would benefit passenger rail. Rail security is significantly underfunded as compared to the expenditures for other modes of transportation.[91]

Richard Falkenrath, the New York City Police Department's Deputy Commissioner for Counter-Terrorism, has lamented that the field of homeland security has been gripped by a mania for plans, strategies, and other reports.[92] Of particular concern are the reports mandated by the federal government, often as a condition for receiving grant funding. They are of almost no value to the field and reflect the watered-

---

87 Waugh, "Securing Mass Transit," 310.

88 *Mass Transit: Challenges in Securing Transit Systems: Testimony before the Sub-committee on Housing and Transportation, Committee on Banking, Housing and, Urban Development*, 107th Cong. (7) (2002) (testimony of Peter Guerrero, Director Physical Infrastructure Issues).

89 Waugh, "Securing Mass Transit," 311.

90 Ibid., 4.

91 Plant and Young, *Securing and Protecting*, 55.

92 *Richard A. Falkenrath, Deputy Commissioner for Counterterrorism, New York City Police Department, Prepared Statement of Testimony before The Committee on Homeland Security United States House of Representatives*, 110th Cong. (2007), www.nypdshield.org/public/SiteFiles/documents/DCCTbeforehouseofreps.pdf, 12.

down consensus of participants who have no connection to operational decision making of the most important agencies. Also, Mr. Falkenrath stated that is it unreasonable to expect DHS to generalize about security deficiencies and produce a useful, viable national strategy for securing all U.S. mass transit.[93] These systems are too complex, and federal officials know little about the real world, day-to-day activities of local transit agencies.

## F. EXAMPLES

Passenger rail agencies utilize various methodologies for risk assessment purposes. The primary concern in the past was to address manmade occurrences, such as terrorism. Today, an all-hazards approach, which includes natural disasters, is the standard.[94] The overarching goal is to make informed decisions regarding risk reduction for critical assets. Enhanced security is dependent on the implementation of mitigation strategies, such as infrastructure hardening, but funding for projects is finite. The results of an internal security assessment provide a defensible metric for resource allocation decisions, whether it be funding for supplements to personnel or equipment. An intelligent adversary, intent on damaging a passenger rail system, will exploit opportunities that change the probabilities of the threat. Tactics are ever evolving which, in turn, cause changes to the threat landscape.

Several methods are used to assess the risk to passenger rail systems. A short discussion of these methods and considerations for each method follows.

### 1. Terrorist Risk Assessment and Management Tool

Terrorist Risk Assessment and Management Tool (TRAM) addresses mitigation effort aimed at a range of threats, such as natural disasters and pandemics, but it is weighted heavily toward terrorism. The six-step process, which generates a quantifiable value for an asset, includes criticality, threat, vulnerability, response, impact, and risk.[95]

---

[93] Ibid., 12.

[94] National Research Council, *Review of the DHS Approach*, 58.

[95] U.S. Department of Homeland Security, *Risk Management*, 50.

The results show the comparison of risk among assets based on likelihood and consequence. According to National Research Council in *Approach to Risk Analysis*, TRAM is dependable since it does not rely on subject matter expert (SME) assumptions.[96]

A point to consider in the TRAM methodology is that it is too speculative in nature.[97] The threat analysis component requires the user to rate how attractive various assets might be to a terrorist. It is questionable whether or not a SME could reliably estimate all of these factors and weights from experience since there is such a large, diverse database to interpret. In the DHS report entitled *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, it states,

> A similar process is followed to develop numbers that represent the deterrence associated with each asset. Deterrence factors are aspects such as the apparent security and visibility of each asset. A SME is asked to weigh those factors. The sum for deterrence is multiplied by the target value to arrive at a "target attractiveness" number for each asset.[98]

### 2. Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability Matrix

The criticality, accessibility, recuperability, vulnerability, effect and recognizability (CARVER) matrix is a tool that was developed by the Department of Defense. It includes threat information that identifies different attack methods that could be used by a terrorist.[99] It is a dual function program. From a defensive standpoint, it can determine what targets are more likely to be attacked. Conversely, it can also be used as an offensive aid to decide what assets are vulnerable and susceptible to attack. It employs a scoring system that considers seven attributes of an asset: criticality, accessibility, recovery, vulnerability, effect, identifiability, and impact. A high score signifies that an asset is more vulnerable to attack.

---

[96] National Research Council, *Review of the DHS Approach*, 36.

[97] U.S. Department of Homeland Security, *Risk Management*, 87.

[98] Ibid., 88.

[99] Nuclear Regulatory Commission, *Background Information on Threat Assessments and CARVER Analysis*, last modified June 10, 2015, http://www.nrc.gov/docs/ML0802/ML080280286.pdf.

An issue with the CARVER matrix is that assets are evaluated independently. The program does not generate a matrix with the ability to analyze and compare the risk faced across a group of assets.

### 3. Maritime Security Risk Analysis Model

The maritime security risk analysis model (MSRAM) methodology focuses on target and attack scenarios. According to Stephen Caldwell in a report from the Government Accountability Office,

> MSRAM was designed to identify and prioritize critical infrastructure, key resources and high consequence scenarios using a common methodology, taxonomy, and metrics to measure security risk from terrorism. It assesses risk based on scenarios through pre-determined targets and attack modes and provides quantitative result

There are concerns with MSRAM. Multiple judgments are inherently subjective and constitute sources of uncertainty that have implications. Given the uncertainties in estimating risk reduction, it is unclear if MSRAM provides meaningful performance information with which to track progress over time. In addition, the risk reduction measure is a specific estimate rather than as a range of plausible estimates, which is inconsistent with risk analysis criteria. MSRAM threat information does not account for adaptive terrorist behavior.[100]

### 4. Enterprise Risk Management

The National Research Council discusses enterprise risk management (ERM) in *Approach to Risk Analysis,* noting, "ERM is designed to enable individual DHS agencies, groups or the entire administration to manage risk from multiple perspectives across the mission space. The process seeks to assess risk in a consistent manner from multiple perspectives."[101] Examples include managing across missions within a single DHS component, assessing by hazard type, managing by homeland security function, or

[100] Ibid., 15.

[101] National Research Council, *Review of the DHS Approach,* 52.

managing by security domain. The goal of this approach is to break down stovepipes or silos and manage risk across an entire institution.[102]

ERM may not be an adequate methodology given the circumstances. Although an integrated approach may work well for a government agency or private industry concentrating efforts on one particular sector, the DHS mission is heterogeneous and encompasses a wide variety of complex environments.[103] Attempting to integrate the risk assessment process in response to different threats could be problematic.

[102] Ibid.

[103] Ibid., 84.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. METHODOLOGY

Passenger rail security improvements, like other forms of infrastructure protection, require system operators to assess threats from an attack by an intelligent adversary. Response to a threat results in the development of defenses to deter attacks, or, in the case of a successful attack, to enhance resiliency to mitigate the damage. This approach ensures that resources protect assets with the greatest exposure.

Cathleen Berrick explains that risk management is

> a continuous process of managing risk through a series of actions. This includes setting strategic goals and objectives, performing risk assessments, and evaluating alternatives to reduce identified risks by preventing or mitigating their impact. This results in selecting courses of action to take, implementing and monitoring those actions, and evaluating the results over time.[104]

Within this context, decisions must be made in a cost-effective manner.[105] Risk management involves decision making to select and deploy security measures resulting in an acceptable level of risk at a reasonable cost.

## A. RISK ASSESSMENT

The primary tool for determining the likelihood of an attack is a risk assessment. Boyd and Sullivan define a risk assessment as "a comprehensive study of a transit agency to identify components that are most vulnerable to criminal activity, including acts of terrorism, and to assess the impact of such activity on passengers, employees, and the agency."[106] A risk assessment centers around the question, how bad is it?[107] The result assists security personnel in making critical decisions about allocating resources to protect people and infrastructure. Countermeasures to deliberate threats include visible security presence, physical hardening, mitigation resources, advanced technologies, and

[104] Berrick, *Key Actions*, 19.

[105] David L. Alderson, "Risk and Critical Infrastructure Systems: Practice and Pitfalls" (presented at the Naval Postgraduate School, Monterey, CA, October 2013).

[106] Boyd and Sullivan, *Emergency Preparedness*, 28.

[107] Alderson, "Risk and Critical Infrastructure."

employee training. Some segments of the infrastructure benefit more than others. Optimization techniques are applicable to the decision-making process, but most are of limited use due to the uncertainty surrounding an intelligent adversary's actions. A graphic describing the risk assessment process can be seen in Figure 1 (see appendix).

Uncertainty, a component of any risk assessment activity, is apt to occur in the prediction of future activities and in the analysis of past actions. Uncertainty is an outcome of missing or incomplete information, an inexact understanding of the behavior of people within certain environments, and the inability to develop working models to provide predictions as needed.[108] A resolution process appropriate for risk and threat decision making has been implemented at many transit agencies.

One of the most common ways of calculating risk is through the following equation:[109]

$$Risk = Threat \times Vulnerability \times Consequence$$

*Threat* is the likelihood of a certain attack, *Vulnerability* is the probability an attack will succeed, and *Consequence* measures the damage resulting from a successful attack, such as deaths or cost to replace infrastructure. The framework of $R = T \times V \times C$ is referred to as TVC in the literature. A report to the chair of the Committee on Homeland Security, House of Representatives stated that a risk assessment

> builds upon accepted practice where risk has been equated to the probability of events multiplied by the magnitude of expected consequences. Information from these three elements contributes to an assessment that characterizes risks on a scale such as high, medium, or low and provides input for evaluating alternatives and management prioritization of security initiatives.[110]

[108] National Research Council, *Review of the DHS Approach*, 140.

[109] Ibid., 15.

[110] Berrick, *Key Actions*, 19.

Security resources distribution must be based risk assessments and not political considerations. The General Accounting Office has evaluated the TVC framework as containing the key elements required for a sound assessment of risk.[111]

On the other hand, the TVC formula may not be satisfactory for calculating the risk from terrorism, since the linkage between these components does not hold.[112] Non-deliberate hazards, such as acts of nature, lend themselves to TVC model because the data that supports "T" exists, whether historical or otherwise. Over time, natural events, such as hurricanes, are going to occur although the specific date and time cannot be known. The certainty of non-deliberate hazards allows for predictions of an expected outcome and modeling of this type of threat.

The components of TVC are not well defined in the analysis of a deliberate threat. The United States has attempted to quantify TVC numbers to develop priorities for defensive resource allocations concerning infrastructure protection. Consequence is not easily specified for interdependent systems, such as passenger rail, because when a system in a major city is rendered inoperable by a terrorist attack, it is difficult to determine the ramifications aside from the impact of the inability for employees to get to work. The economic repercussions, such as the inability to get to work and accomplish other tasks, are enormous. The lack of data prohibits modeling of the deliberate threat.

Another problem with TVC is that the components cannot be separated or influenced independently for deliberate threats.[113] Decisions regarding expenditures for security enhancements affect the nature of the threat by lowering the consequences of an attack. The threat (T) depends on what an attacker knows about an asset's vulnerability (V) and the consequence (C) associated with rendering an asset inoperable. The variable T is dependent on V and C. Defender mitigation strategies are designed to deter an attack. The result could be to deflect it away toward a target that is more attractive due to a

---

[111] *Strategic Budgeting—Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities: Testimony before the Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security, House of Representatives*, 109th Cong. 11 (2005).

[112] National Research Council, *Review of the DHS Approach*, 109.

[113] Alderson, "Risk and Critical Infrastructure Systems."

higher probability of success. Another outcome is to steer the threat to another segment of the same system that is not needed to maintain service at a diminished level.

In *Improving Risk Analysis*, Louis Anthony Cox writes,

> Applying probabilistic risk assessment (PRA) methods to threats from intelligent adversaries may result in severely incorrect and misleading estimates of risks, and in recommendations that fail to reduce them as much as possible for resources spent. Risk estimates based on beliefs about the possible actions of others leads to problems in analysis that cannot be solved by PRA. An approach based on explicitly recognizing that attack probabilities may depend on information that an attacker has, but that a defender does not have, results in useful risk management decisions that are superior to those from PRA based only on our own information.[114]

Unfortunately, estimates based on beliefs about the possible actions of others lead to problems in analysis that cannot be solved by PRA. The threat model approach does not work for intelligent adversaries because there is not enough information to build useful models on deliberate threats.

## B. GAME THEORY

The better option for the risk assessment of deliberate threats is to model the system and then apply a worst-case analysis. This yields well-grounded results, informing the decision maker as to the worst possible outcome, not the most probable one. Game theory principles in the attacker-defender methodology (AD) result in effective recommendations for allocating resources because the foundation of AD is based on improved risk analyses of the actions of intelligent adversaries.

Game theory is the study of strategically independent behavior. It involves decision making wherein participants make choices that impact on the actions of an

[114] Louis Anthony Cox, Jr., *Improving Risk Analysis* (New York: Springer, 2012), 163.

opponent.[115] There has been increasing use of this model in infrastructure security, especially after September 11, 2001.[116] David Alderson argues,

> Game theory, in contrast to PRA, models the actions of interacting 'players' and therefore offers a more appropriate framework for modeling (a) a society that wants to protect its infrastructure from attack by building defenses (b) an adversary who is likely to see those defenses and to attack in a maximally harmful way, and (c) a society that will observe the results of any attacks and operate to the best of its reduced ability. We propose such a model here, with the goal of maximizing resilience of infrastructure, i.e., minimizing disruption, against worst-case attacks. Disruption is evaluated quantitatively.[117]

The operator acts to mitigate the damage from an attack and to keep the system functioning effectively despite impairment. The goal is to maximize resilience and minimize disruption against worst-case attacks, which minimizes the disruption caused by worst-case attacks.

Game theory models the actions of "players" and offers a more useful modeling framework than other risk management approaches. These players include a society that wants to prevent attacks against its infrastructure, adversaries who recognize protective measures and seek to attack in the most harmful way, and a system that bounces back and operates to the best of its diminished ability.[118]

The AD model addresses criticality, vulnerability, and threat, albeit not within a probabilistic framework. Protection, such as target hardening, aims at preventing damage since each segment of the system is prone to an attack. Threats are mitigated by allocating resources to counter the terrorist(s). The analysis determines the criticality of an asset, which relates to the cost of protecting it, and the value that results from system redundancy can be calculated as well.

---

[115] Theodore L. Turocy, "Game Theory," in *Encyclopedia of Information Systems* (Academic Press, 2002), 2.

[116] Vicki M. Bier and Sinan Tas, "Game Theory in Infrastructure Security," *WIT Transactions on State-of-the-art in Science and Engineering* 54 (2012): 91, doi:10.2495/978-1-84564-562-5/06.

[117] Alderson and Brown, "Solving Defender-attacker-defender Models," 29.

[118] David L. Alderson and Gerald Brown, "Solving Defender-attacker-defender Models for Infrastructure Defense" (paper presented at the 12th Informs Computing Society Conference, Monterey, CA, January 2011).

Because it is not possible to deter all terrorist attacks, success is measured by the ability to keep the system operating (this is a factor in defining resiliency). In the past, operators designed infrastructure to avoid single points of failure. However, these systems may not survive an intentional, malicious attack or an attack against multiple, simultaneous targets.[119] Alderson reiterates,

> according to the U.S. National Strategy for Homeland Security, the infrastructure mission is to focus on the resilience of the system as a whole—an approach that centers on investments that make the system better able to absorb the impact of an event without losing the capacity to function.[120]

The system acts to mitigate the results of any attack and operates to the best of its reduced ability. The goal is to maximize resilience and minimize disruption in worst-case attacks.[121]

The ability of an attacker to adapt to circumstances is taken into consideration in the AD methodology. In this interdiction model, one player acts to preserve system operability while the other interdicts to cause disruption. Behavior is a decision and not a random event. It is possible for the user of this methodology to act as defender or attacker and gain the perspective from either side to identify gaps.

In his article, "Game Theory and Risk Analysis," Anthony Cox states there are three actors in this model:

1. The Operator is intimate with how the system functions and understands what the worst-case scenarios are that would debilitate transportation vitality. The operator routinely deals with disruptions and develops processes to minimize the impact. These include instances such equipment failures, adverse weather, and bomb threats. In response, the operator has alternatives, such as re-routing assets to keep the system running.
2. The Defender, who has limited resources, is responsible for minimizing the damage from an attack and ensuring that the system keeps running despite disruptions.

---

[119] Gerald Brown and Matthew Carlyle, "Defending Critical Infrastructure," *Interfaces* 36, no. 6 (2006): 530.

[120] Alderson and Brown, "Solving Defender-attacker-defender Models," 1.

[121] Ibid., 29.

3. The Attacker is intent on damaging a system and takes into account the defender's security resources. The attacker's actions expose vulnerabilities, which test the system's resiliency.[122]

This model works on the following assumptions. Player behavior is a decision and not a random event.[123] Each player receives a consequence, such as people killed or injured, property destroyed, psychological harm, or lifestyle disruption. The attacker can see the defender's security allocations, but the defender has no knowledge of the attacker's preferences.[124] Strengthening one location makes it more attractive to attack another. Both sides want to find the best strategy to employ against the opponent. Furthermore, the model assumes "perfect knowledge," wherein the attackers know everything about the potential targets and defenders know everything about the attacker's capabilities. While this is not the case in practice, it does conform to the "worst-case" principle of the methodology.

Variables come into play. For instance, timing in simultaneous games involves players selecting alternatives without knowing the actions of the other players. In sequential games, which are also called attacker-defender games, the attacker moves first, followed by the defender, who moves after observing the actions of the attacker. The leader has the advantage since the choices he or she makes limit the options available to the follower.[125] Infrastructure security decisions are most often modeled as sequential games, since an attacker can observe defensive investments before choosing a strategy. On the other hand, decisions can be changed and may be modeled as a simultaneous game.

The game involves complete information if the actions are common knowledge to all players. When information is not common knowledge, it is a Bayesian game, a game in which players only have information about the preferences of other players.[126] In a

---

[122] Louis Anthony Cox, "Game Theory and Risk Analysis," *Risk Analysis* 29, no.8 (2009): 1062.

[123] Alderson, "Risk and Critical Infrastructure Systems," 80.

[124] Vicki M. Bier, "Choosing What to Protect," *Risk Analysis* 27, no. 3 (2007): 607.

[125] Bier and Tas, "Game Theory," 2.

[126] Vicki M. Bier, Louis A. Cox Jr., and M. Naceur Azaiez, "Why Both Game Theory and Reliability Theory are Important in Defending Infrastructure against Intelligent Attacks," in *Game Theoretic Risk Analysis of Security Threats*, ed. Frederick S. Hiller, 1–11 (New York: Springer 2009).

game of perfect information, players know all past moves. If the game involves imperfect information, a player does not know all past moves of the other players. In equilibrium, the defender may leave an asset undefended, even if the risk can be reduced through minimal expenditures.[127] These basic concepts are instrumental in developing strategies in which defenders act first, attackers follow, and each succeeding player apprised of the other's actions. The optimization principle comes into play in the attacker's response in deploying resources. In the previous round, the most effective deployment of defensive resources can be determined by considering the attacker's best response.[128]

Though integral for identifying terrorism threats, risk analysis does not follow a standard methodology resulting in recommendations for improvements.[129] Risk analysis revolves round static threats. Infrastructure protection against intentional acts is not like protecting against acts of nature. Moreover, methods for safety analysis are not sufficient for security purposes. An inaccurate estimate of the benefits of security improvements may result if an analysis is performed with an identical threat and assumptions that enhancements have been implemented.[130] Intelligent adversaries change their tactics to defeat security and exploit any vulnerability. Risk assessment models support game theory by providing probabilities for various attacker-defender actions.[131] Game theory is superior to other risk management approaches, which fail to consider the tendency of terrorists to react to defender strategies.

In "Game Theory in Infrastructure Security," Vicki Bier says,

> Among the approaches for defending against intentional threats, game theory models stand out for their mathematical depth. This method anticipates that the attacker will exploit paths of least resistance, rather than acting blindly or randomly in response to defender preparations. Treating attackers as optimizers who calculate best responses to different defensive configurations can lead to different resource allocations, and larger risk reductions, than could be achieved using models that ignore the

[127] Ibid.

[128] Cox, "Game Theory," 1063.

[129] Bier, Cox, and Naceur Azaiez, "Why Both Game Theory," 12.

[130] Ibid.

[131] Cox, *Improving Risk Analysis*, 173.

> ability of intelligent attackers to adapt their plans as information becomes available before and during the course of an attack.[132]

An important consideration concerning the value of utilizing AD is the reliability of threat information. The data to support threat assessment is summarized into categories, such as expert opinions from intelligence analyses, simulations, historical data, research into terrorists' behavior, journalist accounts, and terrorists' literature outlining motivation and intent.[133] Some categories, such as domestic attacks, result in information developed by subject matter experts, which has limitations such as bias, false conclusions, lack of training, and inconsistent estimates.

Game theory has shortcomings. It relies on assumptions, such as an attacker's beliefs about structures and payoffs, which may not be sound when applied.[134] Also, it may ignore the psychological factors that influence actual behaviors. Counter-terrorism risk assessments require input on sociological factors that are not understood very well.[135] Some models generate levels of mathematical sophistication for attackers and defenders that result in improbable predictions for actual attacks and defenses.[136]

## C. FAULT TREE ANALYSIS

The inclusion of the fault tree analysis (FT) can improve understanding of the vulnerabilities that confront the passenger rail industry. This methodology seeks to understand how systems can fail and to find better ways to reduce risk. The model is used to identify, isolate, and correct causes of an undesired event. FT as a supplemental tool highlights the damage identified through other methods, such as a hazard analysis. In addition, it complements the AD methodology by determining the likelihood that a particular attack may occur. This can have a direct impact on the deployment of security resources.

---

[132] Bier, Cox, and Naceur Azaiez, "Why Both Game Theory," 12.

[133] Alderson, "Risk and Critical Infrastructure Systems."

[134] Bier, Cox, and Naceur Azaiez, "Why Both Game Theory," 7.

[135] Ibid.

[136] Ibid., 9.

Joseph Flaus states that FT was developed to assess the risk involved with critical systems, such as intercontinental ballistic missiles and the operation of nuclear reactors. It consists of a top-down structure and represents a model of the pathways, which leads to an undesired state, such as failure or loss of a system. The symbols are labeled as events, gate, or transfers.

- Events—used for primary events such as basic, external, undeveloped, conditioning, or intermediate events.
- Gates—the relationship between input and output events
  - OR gate—the output occurs when any input occurs
  - AND gate—the output occurs when all inputs occur.
- Transfers—used to connect the inputs and outputs.[137]

FT models are deductive, and the steps proceed in order. First, the event requiring resolution is defined and broken down into causal events. Causal events signify failures, which occur in a certain progression. The step-by-step resolution leads to subsequent events, which continues until basic, primary causes are identified. Appropriate logic is employed to show event relationships. One of the benefits of FT is it provides a framework for a through quantitative or qualitative evaluation of the top event. This results in identification of effective upgrades to the system to address causes of the failures. This is directly linked to the optimization of resources to be expended to enhance security.[138] See Figure 2 for an example of a fault tree analysis (see appendix). It outlines the causal events behind a non-security related problem—the inoperability of a passenger train. Though simplistic, it exposes the root causes of the failure and ultimately leads to the primary events. Identification of the possible causes provides actionable information to prevent future occurrence.

The first step in the methodology is creating the operator's model. This describes how the system works—how does it provide the service of function for which it was built? The parameters within the operator's model that must be determined up front:

[137] Flaus, *Risk Analysis*, 236.

[138] Ibid., 230.

- What is the system?
- How is performance measured?
- How do parts of the system work together to achieve the operational goal?
- What actions are available to the operator to maintain performance?

The operator's model provides a foundation for performing the analysis through the context of a previously defined methodology. A passenger railroad consists of steel rails, which are held a fixed position on a right of way. Trains, which are often referred to as cars or vehicles, are connected together, guided by flanged wheels, and propelled; the result is transportation. The intention of modeling an infrastructure system is not to determine the importance or value of an asset; rather, it models the value that the system represents to society, how loss of components reduces the value, and how improvements prevent loss of value.[139] The meaning of value revolves around the system under consideration. In this case, passenger rail equates to economic output, the movement of people, which in turn results in prosperity and economic value. Passenger rail systems move people from one point to another. In locations wherein systems operate, development occurred due to factors such as need, political support, and finances. Patrons will support a system if it accomplishes the goal of transporting them to a place that they want to go safely and efficiently.

The operating philosophy of passenger railroads ensures that the system can sustain significant damage and continue to function.[140] Moving away from a network based on robustness to one that reinforces resiliency is a strategic shift because systems are currently designed to prevent failures. In many cases, the result of this has been increased complexity that engineering to higher standards poses to fail-proof planning. A resilient system accepts that disasters will occur and emphasizes early discovery and prompt recovery from failure.[141]

---

[139] Gerald Brown and Matthew Carlyle, "Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses," in *Tutorials in Operational Research*, ed. J. Cole Smith (Catonsville, MD: INFORMS, 2005), http://pubsonline.informs.org/doi/book/10.1287/educ.1053, 104.

[140] National Research Council, *Deterrence, Protection, and Preparation*, 52.

[141] National Infrastructure Advisory Council, *Sector Resilience Report: Transportation—Passenger Rail* (Washington DC: National Infrastructure Advisory Council, 2015), 5.

Passenger railroads, like most other infrastructure systems, are engineered to handle disruptions and anticipate some degradation in performance. Railroads have emergency response and preparedness plans and continuity of operations protocols that have been implemented in real-time situations to avoid a total shut down. Operators make decisions related to system activities to keep trains moving to the highest capacity possible given the circumstances. Within the rail system, there are frequently disruptive events of different magnitudes, such as suspicious items on trains or in stations requiring investigation. The application of contingency procedures in response to a given event, such as a hurricane resulting in extensive flooding, provides benefit to the rail agency. It keeps the staff attuned to the host of actions necessary to maintain service under dynamic circumstances and provides the opportunity for after-action analysis. Reflecting on past actions to identify accomplishments and shortcoming is key to not only to improving future performance but responding to unexpected disruptions that terrorism can bring.

In the all-hazards context, whether the event is manmade, like a terrorist attack designed to cripple an internet service, or natural phenomenon like a hurricane that inundates a power distribution system, the intent of resiliency and continuity of operations protocols is to keep some segment of the system functioning while restoration efforts proceed to bring the entire system back to a state of normalcy. The limits on capacity depend on the features of a particular system.

Networks have a built-in level of redundancy, such as several lines that may parallel each other. This feature allows for continuity of service under adverse conditions. A system that operates 24 hours a day, such as the NYCT, has been tested many times in the past by events such as severe storms. The mass transit systems needing the most security have the most to lose— in an operational context. New York City could not maintain its vitality without a fully operational subway system. This is one reason why a municipality like New York is such a high-risk target.[142]

Other systems that offer limited service are not as robust and have a lower threshold of resiliency. When stressed, service can be completely disrupted. As well

[142] Armstrong et al., *Securing America's Passenger Rails*, 42.

prepared as NYCT is, it too has limits. A single point of failure, the Achilles heel of any passenger rail operation, is power distribution. Railroads have no ability to produce or store electricity. As seen during the Northeast Black-out of 2003, interruption of the power supply resulted in total loss of the system. Security professionals monitor these single points of failure closely to implement defenses to reduce the likelihood of failure caused by intentional acts, such as terrorism.

Passenger railroads serve large areas. For instance, the service territory for the New York Metropolitan Transportation Authority's Metro-North Railroad covers 2701 square miles in the states of New York and Connecticut.[143] Systems are expected to protect riders and provide security coverage over the entire system. Due to limitations on personnel and funding, it is not practical to provide the same level of protection across the entire network; operators must make choices about which technologies or techniques to use. Systems employ layers of security across the network, which vary in concentration from one part of the system to another. Many factors must be considered when deciding where to expend resources. Operators prioritize these factors based on factors including criticality, ridership, and iconic value. Additionally, operators must make choices about which technologies to employ. Security personnel have not adopted the mantra, "We can't cover it all," but provide coverage from line to line and station to station as needed. Security enhancements are implemented at different levels across the system. Decisions on where to apply resources lead back to the assessment process. Improvements, such as closed circuit television, are expensive. With limited budgets, operators cannot leverage this resource across the system. However, other measures, such establishing memorandums of understanding to share resources, are not costly undertakings. Enhanced passenger security awareness programs, such as the DHS "See Something, Say Something" initiative, are not expensive to implement and can be more widely distributed throughout a system.

[143] Metropolitan Transportation Authority, "Metro-North Railroad Information," accessed June 27, 2016, http://web.mta.info/mnr/html/generalinformation.html.

## D. MEASURE OF PERFORMANCE

A measure of performance (MOP) is the degree to which a system performs. MOPs supply supporting data to determine measure of effectiveness. MOPs evolve over the life of a program and determine what constitutes successful operation for the system. Their selection should be based on the ability to discriminate between levels of good performance. An effective MOP measures "perfect" performance wherein the system is running optimally, as opposed to a degraded performance after some accident, attack, or even planned outages during which the system is operating at less than an optimal level. Performance measurements are incorporated in all aspects of a system, including design, building, operation, and maintenance. For example, in the design phase, MOPs can be of physical properties. In maintenance, they revolve around repair, reliability, or downtime.

The MOP that attackers may consider to measure the effectiveness of activities, such as bombings or mass shootings, is subject to interpretation. It may not necessarily be a widespread disruption of the system. Recent trends indicate that terrorist attacks are increasingly focused on racking up high body counts.[144] Most system operators have adopted a policy of completely shutting down after an attack occurs. While this action minimizes the potential for further loss of life and destruction of property by permitting the methodical recovery processes to clear the system of any additional threats, it imposes a major disruption on a large segment of a population. Such actions have a vast impact on society, which is the intent of the terrorist. One of the intangible aspects is the psychological effect that results from the public's reluctance to use a passenger rail system after such an event. System operators can reduce the ridership's apprehension by maintaining a high level of resiliency. However, terrorist's effectiveness of instilling fear into a populace cannot be completely measured by how many patrons decline to use a system after an attack, since a limited number of people ride the rails.

Judging by statements that terrorists make regarding their motivation for committing atrocities, economic damage, disruption, and instilling fear broadly among

[144] Brian M. Jenkins and Bruce Robert Butterworth, *The Deadliest Bomb Attacks: The Most Lethal Combinations, 1975–2015* (San Jose: Mineta Transportation Institute, 2007), 9.

the populace are central to their efforts.[145] Based on trends from past incidents, the MOP that attackers consider is the potential for achieving injuries and deaths.[146] Since passenger rail transportation hinges on complex networks that have the ability to absorb disruption and keep on functioning, a system shut down is almost impossible to accomplish even by means of an extremely devastating attack. There are single points of failure, but they would require sophisticated tactics to achieve a system shutdown.

As Wilson, Jackson, and Eisman state in *Securing America's Passenger Rail Systems*,

> The threat of terrorism to rail systems must have as its basis information, not just on types of attacks, but also on the consequences of attacks when they occur. This understanding should be based not just on the casualties produced by attacks, but also on the physical damage caused and the incident's effect on rail system functioning. Not enough data is available to support a systematic assessment of all of the consequences of terrorist attacks.[147]

A common MOP that passenger rail system operator's use is on-time performance.[148] Passenger rail, unlike freight rail, is time sensitive. People patronize passenger rail to travel promptly from one point to another. While operators will not sacrifice safety for on-time performance, this MOP is used as an indicator of efficiency. In the security field, crime statistics provide a MOP that drives the prioritization of resources, including personnel deployments, technology procurements, and adjustments to processes and procedures.

Defenders take actions to mitigate worst-case scenarios. The actions seek to counter the MOPs that an attacker can exploit and minimize any decrease to the defender's MOP. When system operators defend against the worst-case scenario,

---

[145] U.S. Department of Homeland Security, *Continuing Terrorist Interest in Subway and Passenger Rail Systems* (Washington DC: Office of Intelligence and Analysis, National Protection and Program Directorate, 2007), 3.

[146] Ibid., 43.

[147] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, 35.

[148] William Vantuono, "Hurricane Sandy Devastates NY/NJ-Area Passenger Rail Systems," *Railway Age* 213, no. 10 (2012), http://www.railwayage.com/index.php/passenger/commuter-regional/hurricane-sandy-devastates-ny-nj-area-passenger-rail-systems.html.

associated actions have the ancillary benefit of mitigating intermediate threats. For instance, enhanced security presence, such as uniformed personnel supplemented with canines and heavy weapons, deters active shooter attacks. This defense also has an effect on preventing trespassing. The entire system realizes a benefit when operators implement a particular security feature.

The worst-case scenarios, which cause the greatest disruption, can be attributed to natural events. In 2012, Hurricane Sandy had an enormous effect on New York-New Jersey passenger rail systems and resulted in system-wide service outages for over a week. This impacted millions of people in the region who depend on passenger rail. The damage required billions of dollars to repair.[149] In addition, the New Jersey Transit Rail Operations Center was inundated, which destroyed backup power supply systems and the network that controlled train movement. Furthermore, the damage from high winds and the storm surge was extensive, and flooding alone significantly impacted to over 500 miles of track. Even though 85 percent of NYCT was running within a week of the storm, officials stated that it would take years to return the system to pre-hurricane conditions.[150]

On the other hand, manmade threats, such as bombings, also have the potential to cripple passenger rail systems. The 2005 London subway bombings succeeded in shutting down the system for 12 hours, and the NYCT was completely shut down for three days after the 9–11 attack on the World Trade Center. However, unlike in the case of natural forces, such as storms, service did not cease because of the damage the explosions caused to the infrastructure. These shutdowns were purely precautionary move. The operators were concerned that there were more IEDs on the system, which meant that passengers might be in danger. Procedures were instituted to immediately suspend service, evacuate all trains, and close the system, which allowed for a sweep of the network to ensure that the danger had passed.

[149] Ibid.

[150] Cotey, "For New York, New Jersey Transit Agencies."

Passenger rail operators can take actions on several levels to mitigate threats. Security measures appear to work primarily as a deterrent. Deterrence is difficult to measure for events that do not occur and cannot be counted. Terrorist events are rare and statistically random, making it difficult to connect patterns of events with specific security measures.[151] There is some evidence that increased security measures implemented on London's tube and train stations during the Irish Republican Army's bombing campaign of the 1970s gradually drove attackers away from their preferred high profile targets in central London. These measures included increasing television surveillance, the enlistment of the public in calling attention to abandoned parcels, and rapid response by the authorities.[152]

One of the most effective countermeasures to terrorism has been good intelligence.[153] Intelligence has enabled authorities to uncover and thwart potentially deadly attacks. Federal, state, and local law enforcement agencies, and the intelligence community, must continue to share information and expertise. The connectedness of public transit systems makes the formation of partnerships between various law enforcement agencies essential. In a small but significant percentage of attacks, someone acted to stop an attack before it could be completed. The security system, defined broadly to include alert transportation employees and the public, has prevented some plots from occurring.[154]

While process-based improvements, such as personnel deployments, feature prominently, operators are not totally reliant on this type of frontline security enhancement. Planning and design can incorporate the principles of a process known as crime prevention through environmental design (CPTED).[155] CPTED creates physical conditions through environmental design in venues to reduce crime. CPTED uses a two pronged to addressing security issues: suppressing opportunities for undesirable activities

[151] Jenkins and Butterworth, *Analysis of Terrorist Attacks*, 8.

[152] Ibid.

[153] Sahm, *Hard Won Lessons*, 9.

[154] U.S. Department of Homeland Security, *How Security Personnel*, 1.

[155] Volpe National Transportation Systems Center, *Transit Security Handbook* (Boston: Federal Transit Administration, 1998), 54.

and eliminating "negative space" (areas that promote illegal activity). Opportunities deal with the situational aspect of crime, rather than what drives the offender. Terrorism can arguably be called an extreme level of criminal behavior, so CPTED can be applied to it.

A budget requires an agency to choose how to protect the system, which dictates the defenders model. A rail system operator must consider the costs of acquiring the enhancements vis–à–vis the decreased likelihood of an attack. Wilson, Jackson, and Eisman have outlined the considerations, including:[156]

- The investment cost, which is an estimate of the one-time expenditures for procuring, testing, and installing the security measures.
- The annualized, recurring cost, which is an estimate of the average annual
- Expenses for personnel, training, maintenance, and upkeep of employing the security measures over their expected lives.
- The marginal annual cost is the annual life-cycle cost (based on a five-year time horizon) that accounts for both investment and recurring costs.

Return on investment (ROI) is the ratio of the cost of an improvement to the risk reduction associated with that improvement, and it is calculated to determine if funding is spent in an efficient manner. ROI can also be defined as the ratio of the cost of an improvement to the risk reduction associated with that improvement. Although the estimates of ROI are readily available for various enhancements, the benefits related to anti-terrorism are more difficult to measure. There are two outcomes: decreased odds of an attack or prevention and decreased consequences of an attack or mitigation.[157]

Resilience, or the level of service that a system desires to maintain after a disruption, has a bearing on the security improvements that an operator desires to adopt. Expenditures for various security initiatives correlate to a maintaining a percentage of functionality. This varies, but it may be on the magnitude of 60 percent or 75 percent of the system after an attack that has the potential to completely shut down of service. Enhancements to reduce recovery times are more apt to be funded. The goal is the safe

[156] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, 58.

[157] Ibid.

and secure movement of people. Keeping a system operational, even at reduced levels, is paramount to the mission of passenger rail.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. ANALYSIS

This chapter demonstrates the utility of using the attacker-defender methodology to improve security resource allocation decisions that reduce the risk of terrorist attacks in passenger rail systems. The rail transportation sector, both passenger and freight, provides many opportunities for nefarious activity. Some vulnerabilities are shared, such as infrastructure like tracks, bridges, and tunnels. Others, like hazardous chemical transportation in freight rail and train station security in passenger rail, are specific to one mode. This analysis will concentrate on passenger rail, since trends indicate that terrorists prefer to target passenger rail over other surface transportation modes.[158]

This analysis centers on NYCT. As indicated by the data in Table 3, New York City regional mass transit has been the target of more plots than any other system in the United States (see Table 3).[159]

Table 3. Plots Targeting New York City Passenger Rail

| Date | Target |
|---|---|
| July 1997 | A Brooklyn subway station |
| August 2004 | A Manhattan subway station |
| April 2006 | A tunnel underneath the Hudson River |
| June 2008 | A Long Island Rail Road train |
| September 2009 | A Manhattan subway station |
| September 2016 | A New Jersey train station |

[158] Jenkins and Butterworth, *Analysis of Terrorist Attacks*, 4.

[159] U.S. Department of Homeland Security, *Violent Extremists Interests in Attacking Mass Transit and Passenger Rail* (Washington DC: U.S. Department of Homeland Security, 2010).

The magnitude of the NYCT system and the number of passengers it transports make it an appropriate representative for the case study in this exercise. NYCT has the same components that any passenger system needs to be functional, including power facilities, control centers, security apparatus, and infrastructure. Successful application of AD methodology on a network as large as NYCT can make this information relevant to smaller operations. The process presented here can be replicated elsewhere, even though one operation functions differently than another, because they have common vulnerabilities that attackers seek to exploit.

NYCT's domain has concise tolerances. During peak morning and evening rush hours, more than 600 trains are in motion at any one time.[160] Train lines have a limited capacity to handle the ridership. There are two factors to consider. First, each car in a train can handle up to 100 passengers, and station platforms are designed to handle 10 car trains. The other is headway, which is the minimum distance that trains must maintain between each other. Safety considerations, such as speed and braking capabilities, determine the headway on different segments of the system. Headway is a critical condition and is monitored by the signaling system. The system triggers actions, such as braking independent of the engineer, to ensure that specified distances are maintained. Several lines in the system are operating at capacity based on these factors.

AD methodology strives to maintain performance by finding the most effective alternatives given the constraints facing a system. In the context of risk reduction, there are limited choices that an operator can pursue. This develops in an optimization model because of the lack of information, such as historical attack trends. Furthermore, operators have differing views on what represents performance, such as number of customers transported, revenue collected, or equipment in service. The most obvious MOP is through-put or ridership. Table 4 lists the NYCT stations with the largest ridership. The network model in Figure 3 in the appendix highlights the highest ridership stations on the system and their relationship to each other.

[160] Ibid.

Table 4. Top Five NYC Transit Stations for Ridership[161]

| Station | Daily Ridership (Thousands) |
|---|---|
| Times Square | 207 |
| Grand Central Station | 160 |
| Herald Square | 127 |
| Union Square | 108 |
| Pennsylvania Station | 92 |

Because of its size and centrality, the Times Square station is the appropriate facility to assess regarding reductions in service based on different types of attack. Several factors were considered in choosing this station. In addition to high ridership and being a hub where five lines intersect, the Times Square area draws considerable nationwide attention because more than 42 million people pass through it.[162] This makes it the most visited location in the United States.[163] Several attempted attacks in the Times Square area have received wide notoriety, including a bicycle IED in March 2008 and vehicle-born IED in May 2010. A successful rail system attack at the Times Square station would have serious service implications across the rail system, which is apparent when the MOP, throughput, and the interdependency between this station and others are considered.

NYCT's objective is to provide dependable rail transportation for all of its customers, which amounts to approximately 5.6 million riders daily.[164] Circumstances that impact service, such as equipment issues and adverse weather conditions, arise quite frequently. For instance, in 2012, 141 people were struck by trains, resulting in 55 deaths.

[161] Metropolitan Transportation Authority, "New York City Transit Information."

[162] Noah Remnick and Tatiana Schlossberg, "New York Today: Transforming Times Square," *The New York Times*, August 24, 2015, http://cityroom.blogs.nytimes.com/2015/08/24/new-york-today-change-with-the-times/.

[163] Ibid.

[164] Metropolitan Transportation Authority, "New York City Transit Information."

Most were non-criminal acts (suicides), but all forced a suspension of service on the affected line for the investigation and recovery process to conclude. To keep trains moving, NYCT takes actions, such as re-routing over other lines or adding supplemental bus service, to avoid a complete shutdown of service in the area. The operator takes these actions for resiliency purposes: to maintain the highest level of service possible given the extent of the disruption, which is measured by the number of affected lines, expected length of the delay, and location in the system.

NYCT's operational plans are designed to preserve functionality and counter disruptive events with the ability to halt service. When the system suffers a significant disruption, whether it is non-deliberate hazard such as a weather event or deliberate threat like sabotage, after-action results include adoption of policies and procedures to prevent or minimize disruptions from future occurrences. The variety of plans developed by NYCT gives it depth to deal with unforeseen circumstances, since plans already in place can be modified as needed to maintain service.

The worst-case scenario for NYCT differs from that of any other operator because the system has a design, based in the origins of New York City, to support resiliency. Three separate operations, the Independent Subway System, the Inter-Borough Rapid Transit Company, and the Brooklyn-Manhattan Mass Transit System, serviced various parts of the city in the first half of the twentieth century. In some cases, they serviced the same neighborhoods, running adjacent to each other in a competitive environment. Consolidation of these systems under government control in the 1950s linked the lines together. Over the decades, the network has been continually reconfigured to increase efficiency. Even though this resulted in a highly resilient system, there are still attack scenarios that could significantly impede performance.

The attacker has two options to achieve any or all of the goals that terrorist groups strive to attain: mass casualties, instilling fear in the populace, and shutting down the system. The assault can focus on one station and utilize multiple attack vectors, or the plot could target more than one station using the same attack mode. In this case, the measurement of the impact, or how successful the attack is in affecting the MOP, is the

reduction in ridership. The defender is concerned with providing the protection necessary to deter attacks that could affect the MOP.

A mass casualty incident can be a highly emotional event and efforts to defend against such an attack seek to reduce or eliminate the number of deaths that can result from terrorist strikes. Bolstering security processes to suppress attacks also results in a more robust MOP. There are relationships between the concerns for protecting infrastructure, such as the costs, and the psychological effect that injures and loss of life have on the public. Because of the psychological effect, a rider's response to tragedy could lead her or him to make decisions that may be disproportionate to the actual risk. For example, more people are killed in driving accidents than aviation mishaps, but more people are afraid to fly on a plane than ride in a car. Similarly, the risk of injury or death from human error is greater than that posed by terrorist attacks, but customers will refrain from riding passenger trains longer after an attack than they would after an accident involving an engineer falling asleep. The fear that the public experiences results in reduced ridership as there is a reluctance to patronize the system. A death on NYCT, particularly if associated with terrorism, has drastic implications especially on the system's MOP. This length of time that this persists depends on variables such as the level of confidence that the public has in the operator to restore safe, secure service. Another variable is the availability of alternate modes of transportation. There may be few options able to handle the capacity of a passenger rail system that riders could use in the interim. A better decision making methodology can help passenger rails systems to prepare, mitigate, and recover from infrastructure damage as well as reduce the deep-seated effects that violent deaths have on the populace.

The following sections provide details related to the two attack scenarios, multiple modes—single station and single mode—multiple stations.

## A. MULTIPLE MODES—SINGLE STATION

This plot involves attacking one station simultaneously by different methods. The three most common attack methods are[165]

[165] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, 32.

- Active shooter situation—individual(s) using firearms in an attempt to indiscriminately kill passengers.
- Sabotage—intentional damage or vandalism, such as power outages or derailments to disable a system.
- Improvised explosive device—explosives detonated in a system to kill passengers and destroy infrastructure.

Whether one, two, or all three modes are successful, the attack at the Times Square station could result in a potential daily ridership loss of 206,000 passengers who would be unable to use the station. This equates to a reduction in the MOP of approximately 3.5 percent.

## B. SINGLE MODE—MULTIPLE STATIONS

In this scenario, a single method is directed simultaneously against several stations. An IED plot was selected because it represents the most common type of attack against passenger rail.[166] If attacks at the three busiest stations are successful, they could yield a loss of access to the system for approximately 207,000 passengers at Times Square, 160,000 at Grand Central, and 127,000 at Herald Square. The reduction in the MOP equates to 3.5 percent at Times Square, 3.0 percent at Grand Central, and 2.5 percent at Herald Square, for a total of approximately 9 percent.

If IED attacks were launched simultaneously against the stations, the damage would be structural in nature due to blast effects. Depending on the severity of the attack there could be also be impacts on adjoining stations. Additionally, trains on unaffected lines serving these stations would attempt to bypass the attack zone and remain in service, if the stations were structurally sound. If the damage was great enough to halt service on any line passing through these stations, further reduction to the MOP would depend on which lines were affected. Table 5 was compiled from individual ridership data, for each station along the specified lines, to calculate the percentage of ridership that these lines handle daily. This represents the level of ridership that could be disrupted if an attack on a particular lining running through Times Square was successful in terminating service along the entire length of the route.

[166] Jenkins and Butterworth, *The Deadliest Bomb Attacks*, 46.

Table 5. System-wide Percentage of Ridership on Select Lines[167]

| Line | Total System Ridership Percentage |
|---|---|
| A-C-E Line | 25 |
| 1-2-3 Line | 22 |
| N-R-Q Line | 20 |
| 7 Line | 9 |
| S Line | 4 |

The MOP is adversely affected in a cascading manner as the IEDs increase in force. Coordinated, simultaneous IED attacks against Times Square, Grand Central, and Herald Square, under the worst-case scenario, could result in a shutdown of service on the lines serving these stations, which would affect many more stations up and down individual lines.

A terrorist considers the most effective methods when planning an attack. In the multiple modes—single station attack, there is the potential for shutting down all five of the lines intersecting Times Square in one attempt. Some of the methods, such as sabotage, may not succeed, but if the IED component performs well, the goal of crippling the system is attainable. If the attack hinges on the single mode—multiple station option, all of the attacks must be successful to achieve the maximum impact on the MOP. There is a lower probability of this happening, considering all of the variables involved at several sites.

Both types of attacks, the multiple modes—single station and the single mode—multiple stations, have pros and cons regarding potential for success. The single mode—multiple station attack may have a lower threshold for failure because it has fewer details to coordinate, such as ensuring that attack times are simultaneous. In contrast, the multiple mode—single station attack poses challenges, such as familiarization with the

[167] Metropolitan Transportation Authority, "New York City Transit Information."

structures and possible security interference. Based on the reduction in the MOP that each type of attack could optimally achieve, the single mode—multiple station attack has the potential to produce a more damaging blow to the operator.

What are the most serious threats? The scenarios considered have to be both important and plausible. For instance, a cyber-attack on passenger rail is defined as high-threat/low probability event. It would certainly have the potential to shut down operations. However, historically, there have been no attacks of this type in the sector. Considerations in the identification of scenarios include likelihood, vulnerability, criticality, threats, and history. These generate estimates regarding an adversary's capability to carry out specific attacks. The lack of dirty bomb and chemical dispersal attacks world-wide also places these types in the category of high-threat/low probability attacks.[168]

In *Securing America's Passenger Rail Systems*, Wilson, Jackson, and Eisman reference the RAND-MIPT Terrorism Incident Database (National Memorial Institute for the Prevention of Terrorism and RAND Corporation) and state,

> The most prevalent threat to rail comes from bombings. Attacks in densely packed rail cars and inside of rail facilities are of particular concern because of the casualties they can produce. Not all terrorist attacks on rail systems come from explosives, so security measures must address explosive devices but also appropriately incorporate the possibility of rarer attack modes. In addition, given the damage associated with a relatively small number of large attacks, security measures that prevent only the largest-scale attacks could significantly reduce the human costs associated with this threat.[169]

The defender has options to prevent attackers from inflicting damage against the system. The goal is to identify assets to improve security under the constraints of a limited budget. A report released by the American Public Transportation Association entitled, *Survey of United States Transit System Security Needs and Funding Priorities:*

---

[168] U.S. Department of Homeland Security, *Mass Transit Modal Threat Assessment* (Washington DC: U.S. Department of Homeland Security, 2013).

[169] Wilson, Jackson, and Eisman, *Securing America's Passenger Rail Systems*, 32.

*Summary of Findings*, identified "five security-related capital investments as those for which federal funding is very important." They are[170]

- Radio communications systems
- Security cameras onboard trains
- Controlled access to facilities and secure areas
- Security cameras in stations
- Automated vehicle locator systems

Security enhancements can be grouped into three categories:

- Process based
  - Visibility patrols
  - Security awareness

    Passengers, signage, announcements

    Employees' training
- Technology based
  - Closed circuit television
  - Chemical, biological, radiological, nuclear detection
  - Perimeter intrusion detection systems
  - Access control
- Facility improvements:
  - Blast resistant trash receptacles
  - Bollards

The supposition that single mode—multiple station attacks have the potential to result in more debilitating effects on the MOP points system security staff in a particular direction regarding resource allocation decisions. High volume, iconic stations should be one of the top priorities when it comes to security improvements. Smaller stations on the periphery of the network are not critical to maintaining operations should they be shut down for any reason. However, this rationale does not restrict facilities with low ridership

[170] Peterman, *Passenger Rail Security*, 29.

from receiving security enhancements. Some initiatives, such as closed circuit television and access control, are system based and easily incorporated into a station that already has network capabilities from other processes such as fare collection or public announcements.

The strategies an operator can leverage to counter the effects of an attack, maintain the system's viability, and support a vigorous MOP include redundancy, re-routing, and other process features. These actions are continually exercised during routine disruptions in service that occur on a regular basis. Attackers should be presumed to know everything and even have insight into things that the defender does not know. In the chapter, "Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses," Gerald Brown and Mathew Carlyle state,

> Probabilities based only on what a defender knows, rather than on what the attacker knows, can lead to poor risk management decisions. Doing so, can change risk management recommendations from protecting against attack probabilities implied by expert probabilities to hedging against possible attacks based on what the attacker might know. The public interest is better served by redirecting risk management away from using experts to guess where risk might be greatest and toward calculating where targeted investments will most improve the resilience of critical infrastructures.[171]

The comparison of risk estimates based on experts to the information a terrorist might possess is reflective of the difference between PRA for natural hazards and risk analysis, such as game theory, for manmade threats.[172]

## C. CONSIDERATIONS

Unfortunately, some terrorist attacks will achieve the desired objective. Due to the vast number of security improvements that can be employed, compromises must be made. This includes deciding on whether to adopt policies that strive to minimize loses though deterrence and detection strategies as opposed to those that concentrate improving

[171] Brown and Carlyle, "Analyzing the Vulnerability," 120.

[172] Peterman, *Passenger Rail Security,* 171.

protection, response, and recovery.[173] Some may argue that defending against worst-case scenarios leaves a system vulnerable to less than worst-case threats. However, this philosophy has the opposite effect. Defending against an attack resulting in a reduction to the MOP short of total shutdown is less than the worst-case event and has ancillary benefits.

The effect of security improvements is difficult to determine because defenders may not know that an attack has been foiled. Armstrong agrees, explaining,

> Attacks are rare: as of this writing, no U.S. subway system has been successfully attacked. A successful improvement will not yield a measurable result since the best possible result—zero attacks—has been achieved. Analyzing the probability of an event that has not previously occurred requires advanced methods that are more difficult to interpret. The benefit of a particular security choice is also linked to the cost of a terrorist attack which is difficult to measure. Costs can be determined through a multitude of variables including human death tolls, dollars of physical property damage, and economic loss, among others.[174]

Uniformity in the decision-making process is important to risk reduction because of the connectedness in this sector. If a system is exposed, then all systems are susceptible to an attack.

The knowledge that a terrorist possesses has greater impact on the outcome of an attack than that of the defender.[175] Risk analysis must consider that an attacker, based on input, can alter a plan at any time. Decision makers who rely on probabilistic risk assessment to allocate resources may act on preconceived notions given what is currently known. This is problematic since it does not take into consideration what a terrorist may know at the time of an attack.[176]

---

[173] Ibid., 171.

[174] Armstrong et al., *Securing America's Passenger Rails*, 47.

[175] Cox, *Improving Risk Analysis,* 165.

[176] Gerald Brown and Louis Cox, "How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts," *Risk Analysis* 31 (2011): 197.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. CONCLUSION

The threat that terrorism poses to passenger rail transportation continues even though there has been no significant attack against a domestic carrier. International rail systems suffer attacks, which is why this transportation mode remains at risk. Adversaries contemplate attack methods that will be most effective in damaging the psyche and crippling the economic vitality of our country. A devastating attack against a passenger rail network in a major metropolitan area could happen at any time.

This thesis provides an alternative that passenger rail systems can use to improve resource allocation decisions intended to reduce the risk of terrorist attacks. It began with background information on the influences affecting passenger rail operations, including a review of previous attacks. This thesis includes a review of risk assessment principles along with a summary of various processes to lay a foundation for the analysis and proposed methodology. Game theory, specifically the attacker-defender methodology, has the potential to be the most useful for rail systems to protect against threats from terrorists. At the foundation is a clear, quantifiable measure of performance based on an understanding of how the system works. Modeling of passenger rail systems and the development of measures of performance for these systems creates a common framework for all passenger rail operations. As such, this approach makes for a reliable, reusable tool that rail system personnel nationwide can use in risk assessments for passenger rail systems. Though the particulars may change, the general approach would remain the same.

There are principles that are integral to the attacker-defender model. Due to their structure, some systems are naturally more robust, while others are not. In a game of equal knowledge, the attacker has the advantage. The outcome of an analysis is not always obvious, which helps the practitioner to avoid jumping to risk conclusions. Hardening infrastructure systems to defend against “presumed” attacks can be

prohibitively expensive. Redundancy is often preferable to upgrades that improve component reliability.[177]

Probabilistic risk assessment methodology uses historical data to determine the likelihood that a certain hazard may occur.[178] Given the physical nature of that hazard, one can then design a system to withstand the stresses that it may generate, such as ground motion for earthquakes, wind and wave-slap loading for hurricanes, wind loading and projectile impact for tornadoes, or water levels for floods. In short, natural hazards have historical records that can be used to determine their severity and likelihood.

The same is not possible for an intelligent adversary. Even though, sadly, we are amassing data on terrorist strikes, the very fact that the adversary is intelligent allows the threat to change in real time. An analysis of threat and vulnerability data is difficult because sufficient historical data is non-existent. The attack methods may change as well. An attack against rail network can take advantage of the system's design, and any person passing through a system could be an assailant intent on causing destruction. As such, risk analysis for counter-terrorism is vastly more complicated and less certain than risk analysis for natural hazards.[179]

The challenge is that intentional threats are evolving rapidly, as terrorists respond to defenses. When faced with an intelligent adversary who learns from the past, history offers no security, and the threat data can be too general to eliminate uncertainty. Terrorists are at liberty to change what they attack, when they attack, and how they attack at any point in time. In in *Securing America's Passenger Rails*, Armstrong, Bland, and Cox emphasize,

> The interaction between terrorists and security personnel is a dynamic one in which both sides attempt to gain the upper hand. Assailants study institutional security efforts, systematically probe them in certain

[177] Brown and Carlyle, "Analyzing the Vulnerability," 20.

[178] Bier, Cox, and Naceur Azaiez, "Why Both Game Theory," 150.

[179] National Research Council, *Review of the DHS Approach*, 58.

> circumstances, and attempt to develop countermeasures that will defeat or, disable protective measures.[180]

Instead of using historical data to develop a protective strategy, the attacker-defender methodology engages in worst-case scenarios and develops system models to determine what the worst-case can be. Though this approach does not provide an ironclad prediction, it does frame the solution to what is possible through an attack by an intelligent adversary, and it shows great promise for resource allocation decisions.[181] It is apparent that rail systems have to concentrate on worst-case scenarios in assessing and reducing vulnerabilities because of the lack of confidence in reliability analyses based on unpredictable adversarial threats.

Protecting infrastructure from an attack is extremely difficult. Policy recommendations must take into consideration the limitations of existing authorities and the likely opposition that the proposed protection improvements may face. Therefore, recommendations must be grounded in an understanding of system performance and clearly describe the expected costs and benefits of a particular policy intervention. Furthermore, processes and protocols have to be multi-layered, nimble, and flexible to protect against threats that try to defeat security improvements.

There are additional considerations for passenger rail system operators. They must continue to review trends to ensure that defenses are appropriate for evolving threats. These activities include revising procedures and protocols as needed and updating modeling in threat assessments. In addition, the value of research and development is crucial to developing new technologies that enhance security operations. Moreover, the important role that human capital has in this field cannot be understated. Security is only as effective as the personnel who observe the environment and operable detection equipment. Finally, decisions related to the deployment of security enhancements adopted in a sound step-by-step process are better grounded than those made in crisis situations.

---

[180] Armstrong et al., *Securing America's Passenger Rails*, 47.

[181] Ibid., 106.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX. FIGURES

Figure 1. Risk Assessment Process

Figure 2. Fault Tree Analysis Example

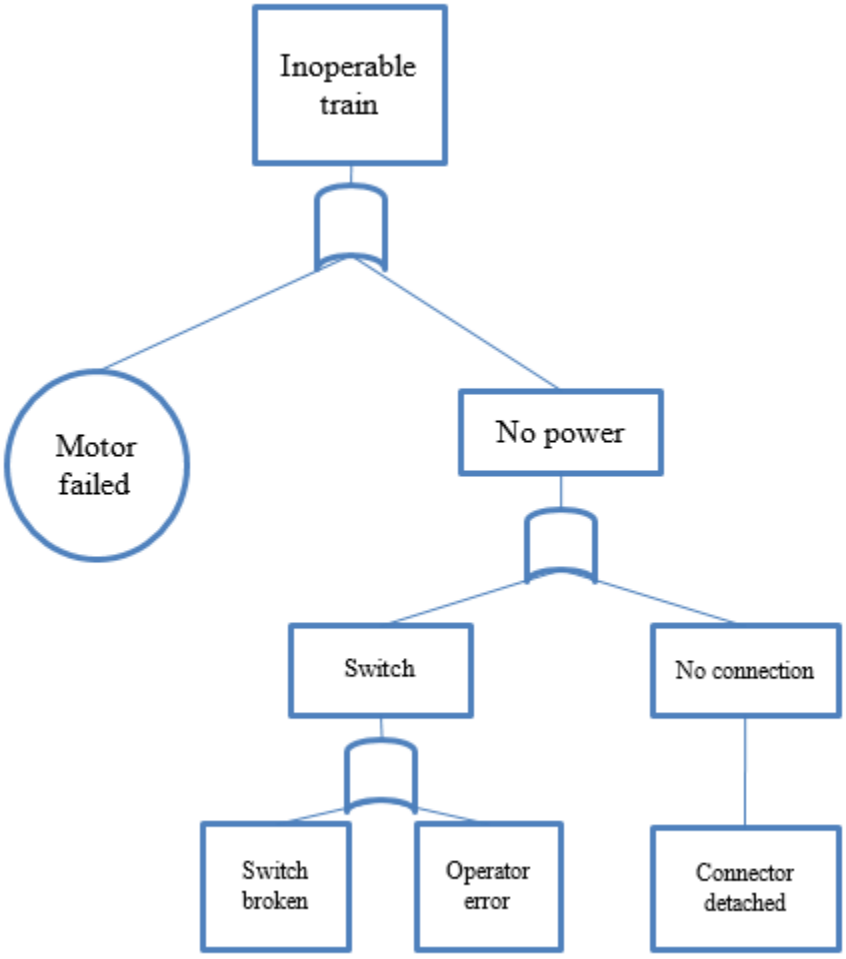
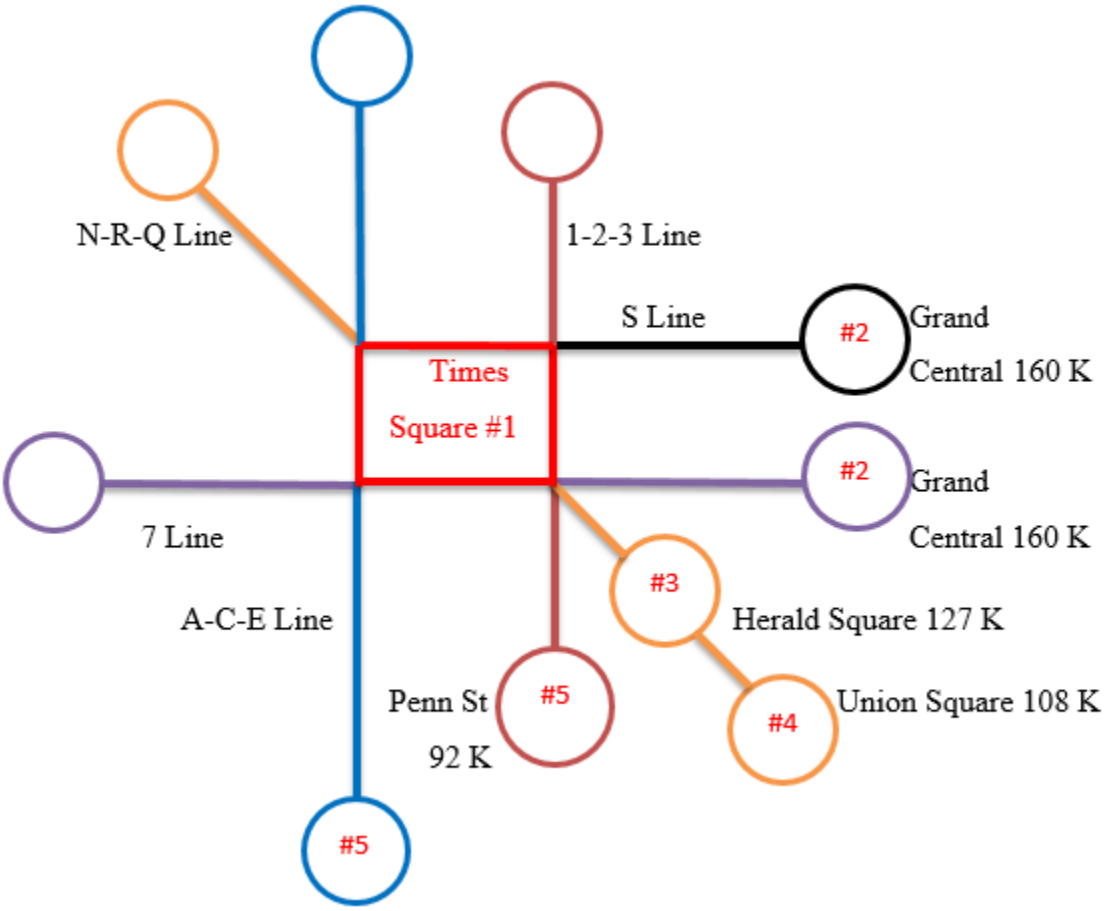


Figure 3. Network Model: NYCT Highest Ridership Stations



THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


Alderson, David L. "Risk and Critical Infrastructure Systems: Practice and Pitfalls." Presented at the Naval Postgraduate School, Monterey, CA, October 2013.

Alderson, David L., and Gerald Brown. "Solving Defender-attacker-defender Models for Infrastructure Defense." Paper presented at the 12th Informs Computing Society Conference, Monterey, CA, January 2011.

Alias, Bart. *Transportation Security: Issues for the 114th Congress* (CRS Report No. RL33512). Washington, DC: Congressional Research Service, 2016.

American Public Transportation Association. *Identifying Suspicious Behavior in Mass Transit* (APTA SS-SRM-RP-009-09). Washington, DC: Enterprise Security Working Group, 2009.

———. *2013 Public Transportation Fact Book*, 64th ed. Washington, DC: American Public Transportation Association, 2013. www.apta.com/resources/statistics/ Documents/FactBook/2013-APTA- Fact-Book.pdf.

———. *Cyber Considerations for Public Transit APTA SS-ECS-RP-001-14*. Washington, DC: Enterprise Security Working Group, 2004.

Armstrong, John. *The Railroad: What It is, What It Does*. Omaha, NE: Simmons-Boardman Books Inc., 1998.

Armstrong, Nicholas, Drew Bland, Edward Cox, Eric Oddo, Dan Wears, and P. C. Zai, *Securing America's Passenger Rails: Analyzing Current Challenges, and Future Solutions* (Syracuse: Maxwell School of Citizenship and Public Affairs, 2008.

Berrick, Cathleen A. *Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*. Washington D.C: Diane Publishing, 2006.

Berrick, Cathleen A., and Jayetta Hecker. *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*. Washington, DC: Diane Publishing, 2006.

Bier, Vicki M. "Choosing What to Protect." *Risk Analysis* 27, no. 3 (2007): 607–620.

Bier, Vicki M., Louis A. Cox Jr., and M. Naceur Azaiez. "Why Both Game Theory and Reliability Theory are Important in Defending Infrastructure against Intelligent Attacks." in *Game Theoretic Risk Analysis of Security Threats*, edited by Frederick S. Hiller, 1–11 (New York: Springer 2009.

Bier, Vicki M., and Sinan Tas. “Game Theory in Infrastructure Security.” *WIT Transactions on State-of-the-art in Science and Engineering* 54 (2012): 91–104. doi:10.2495/978-1-84564-562-5/06.

Boyd, Annabelle, and John P. Sullivan. *Emergency Preparedness for Transit Terrorism*. Washington, DC: National Academies Press, 1997.

Brown, Gerald, and Matthew Carlyle. “Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses.” In *Tutorials in Operational Research*, ed. J. Cole Smith, 102–123. Catonsville, MD: INFORMS, 2005. http://pubsonline.informs.org/doi/book/10.1287/educ.1053.

———. “Defending Critical Infrastructure.” *Interfaces* 36, no. 6 (2006): 530–544.

Brown, Gerald, and Louis Cox. “How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts.” *Risk Analysis* 31 (2011): 196–204.

Cohen, Darryl T. *Population Trends in Incorporated Places 2000–2013*. Washington, DC: U.S. Census Bureau, 2015.

Cox Jr., Louis Anthony. “Game Theory and Risk Analysis.” *Risk Analysis* 29, no.8 (2009): 1062–1068.

———. *Improving Risk Analysis*. New York: Springer, 2012.

Flaus, Joseph. *Risk Analysis: Socio-Technical and Industrial Systems*. Hoboken, NJ: John Wiley and Sons, 2013.

Freemark, Yonah. “Passenger Rail Projects under Way.” The Transport Politic. Accessed September 18, 2016. http://www.thetransportpolitic.com/under-consideration/planned-light-rail-systems/.

International Atomic Energy Agency. *Safety Assessments for Facilities and Activities*. Vienna: International Atomic Energy Commission, 2009.

Jackson, Brian, John Baker and Peter Chalk. *Aptitude for Destruction*. Organizational Learning by Terrorist Groups and Its Implications for Combating Terrorism, Vol. 1. Santa Monica, RAND Corporation, 2007.

Jenkins, Brain M., and Bruce R. Butterworth. *Analysis of Terrorist Attacks against Public Transportation*. San Jose: Mineta Transportation Institute, 2007.

———. *The Deadliest Bomb Attacks: The Most Lethal Combinations, 1975–2015*. San Jose: Mineta Transportation Institute, 2007.

Johnstone, R. William. *Protecting Transportation: Implementing Security Policies and Programs*. Waltham, MA: Butterworth-Heineman, 2015.

Jones, Michael. “Understanding the Terrorist Threat to Underground Rail Networks—Part 1.” *Jane’s Terrorism & Security Monitor* (summer, 1995).

Kennett, Milagros N., Eric Letvin, Michael Chipley, and Terrance Ryan. *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings*. Washington, DC: Federal Emergency Management Agency, 2005.

Lerner, Ben. “Losing Track on Rail Security.” *Homeland Security Today*, April 25, 2016. http://www.hstoday.us/columns/guest-commentaries/blog/losing-track-on-rail-security/fff77b506f8b611b018f4234254a5180.html.

Lord, Stephen M. *Passenger Rail Security, Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*. Washington, DC: General Accountability Office, 2012.

Loukaitou-Sideris. Anastasia, and Brian Taylor. “Rail Transit Security in an International Context, Lessons from Four Cities.” *Urban Affairs Review* 41 no. 6 (2006): 727–748.

Markey, John. *Terrorism Risk for Public Transportation Systems*. NATO Science and Peace for Security Series, Vol. 54. Amsterdam: IOS Press, 2009): 116–144.

Monkkonen, Eric H. *America Becomes Urban: The Development of U.S. Cities and Towns 1780–1980*. Berkeley: University of California Press, 1988.

Morgan, Daniel, and H. Abramson. *Improving Surface Transportation Security Through Research and Development*. Washington, DC: National Academy Press, 2000.

National Infrastructure Advisory Council. *Sector Resilience Report: Transportation—Passenger Rail*. Washington, DC: National Infrastructure Advisory Council, 2015.

National Research Council. *Deterrence, Protection, and Preparation: The New Transportation Security Imperative*. Washington, DC: National Academies of Science, 2002.

———. *Review of the DHS Approach to Risk Analysis*. Washington, DC: National Academies Press, 2010.

Nuclear Regulatory Commission. *Background Information on Threat Assessments and CARVER Analysis*. Last modified June 10, 2015. http://www.nrc.gov/docs/ML0802/ML080280286.pdf.

Pattison, Tony. “The Daegu Subway Tragedy: Was it Avoidable?” *Jane’s Terrorism and Security Monitor*, July 27, 2005.

Peterman, David Randall. *Passenger Rail Security: Overview of Issues* (CRS Report No. RL32625). Washington, DC: Congressional Research Service, 2005.

Plant, Jeremy F., and Richard R. Young. *Securing and Protecting America's Railroad System: U.S. Railroads and Opportunities for Terrorist Threats*. Harrisburg: Pennsylvania State University, 2007.

Remnick, Noah, and Tatiana Schlossberg. "New York Today: Transforming Times Square." *The New York Times*, August 24, 2015. http://cityroom.blogs.nytimes.com/2015/08/24/new-york-today-change-with-the-times/.

Rosenquist, Matthew. *Defense in Depth Strategy Optimizes Security*. Santa Clara, CA: Intel Corporation, 2008. http://www.itworldcanada.com/archive/WhitePaperLibrary/PdfDownloads/Defense_In_Depth_Strategy_Optimizes_Security.pdf.

Sahm, Charles. *Hard Won Lessons: Transit Security*. New York: Manhattan Institute for Policy Research, 2006.

Staes, Lisa, Amber Reep, and Rajesh Chaudhary. *Identification of Cost-Effective Methods to Improve Security at Transit Operating/Maintenance Facilities and Passenger Stations*. Washington, DC: U.S. Department of Transportation, Federal Transit Administration, 2006.

U.S. Department of Homeland Security. *Characteristics and Common Vulnerabilities: Railroad Passenger Stations*. Washington, DC: Protective Security Division, 2005.

———. *Continuing Terrorist Interest in Subway and Passenger Rail Systems*. Washington, DC: Office of Intelligence and Analysis, National Protection and Program Directorate, 2007.

———. *How Security Personnel, Transit Employees, and Passengers Disrupted IED Attacks against Mass Transportation Worldwide, 2004–2010*. Washington, DC: Office of Intelligence, 2011.

———. *Mass Transit Modal Threat Assessment*. Washington, DC: U.S. Department of Homeland Security, 2013.

———. *NPPD at a Glance*. Washington, DC: U.S. Department of Homeland Security, 2014. https://www.dhs.gov/sites/default/files/publications/nppd-at-a-glance-071614.pdf.

———. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*. Washington, DC: U.S. Department of Homeland Security, 2011.

———. *Strategic Sector Assessment: Potential Terrorism Threat to U.S. Mass Transit Systems*. Washington, DC: Office of Intelligence and Analysis, 2006.

———. *Tactics, Techniques, and Procedures Used in the 22 March 2016 Brussels Attacks*. Washington, DC: Office of Intelligence and Analysis, 2016.

———. *Train Station Attack Methods*. Washington, DC: Transportation Security Administration, Office of Intelligence, 2010.

———. *Violent Extremists Interests in Attacking Mass Transit and Passenger Rail*. Washington, DC: U.S. Department of Homeland Security, 2010.

———. *Vulnerability Assessment Methodologies Report*. Washington, DC: Office for Domestic Preparedness, 2003.

Vantuono, William. "Hurricane Sandy Devastates NY/NJ-Area Passenger Rail Systems." *Railway Age* 213, no. 10 (2012). http://www.railwayage.com/index.php/passenger/commuter-regional/hurricane-sandy-devastates-ny-nj-area-passenger-rail-systems.html.

Volpe National Transportation Systems Center. *Transit Security Handbook*. Boston: Federal Transit Administration, 1998.

Waugh, William. "Securing Mass Transit: A Challenge for Homeland Security." *Review of Policy Research* 21, no. 3 (2004): 307–316.

Wilson, Jeremy M., Brian A. Jackson, and Mel Eisman. *Securing America's Passenger Rail Systems*. Santa Monica, CA: RAND Corporation, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California